



JUNOS™ Software

Multiplay Solutions Guide

Release 8.5

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

Part Number: 530-022028-01, Revision 1

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

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

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

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

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

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JUNOS™ Software Multiplay Solutions Guide

Release 8.5

Copyright © 2007, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Mark Barnard

Editing: Ben Mann, Stella Hackell

Illustration: Nathaniel Woodward, Mark Barnard

Cover Design: Edmonds Design

Revision History

12 October 2007—Revision 1

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

YEAR 2000 NOTICE

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

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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.
5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.
8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.
9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.
10. **Taxes.** All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.
11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.
12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.
13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.
14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.
15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

	About This Guide	xiii
Part 1	IPTV Network Solutions	
Chapter 1	IPTV Video Application	3
Chapter 2	Unidirectional Links	27
Part 2	Voice Network Solutions	
Chapter 3	Overview of the Voice Solution	39
Part 3	Index	
	Index	51

Table of Contents

About This Guide	xiii
Objectives	xiii
Audience	xiii
Supported Routing Platforms	xiv
Using the Indexes	xiv
Documentation Conventions	xiv
List of Technical Publications	xvi
Documentation Feedback	xxi
Requesting Support	xxii

Part 1

IPTV Network Solutions

Chapter 1

IPTV Video Application	3
System Requirements	4
Terms and Acronyms	4
Overview and Topology	5
Video Network Elements	6
IGMP and Video Networks	7
IGMP Basics	8
IGMP and Intermediate Devices	8
IGMP Snooping	9
IGMP Proxy	10
DHCP Relay and Video Services Routers	11
Video Networking and the Metro or Core Network	11
What IP Routing Protocols to Use	11
Using MPLS and Label-Switched Paths	12
Redundancy and Failure Detection for Video Services Routers	13
Sample Configuration of an IPTV Network	13
Configuring the Access Side of a Video Services Router Running JUNOS	
Software	17
Configuring the Metro and Core Side of a Video Services Router Running	
JUNOS Software	20
Configuring Router Redundancy	22
Verifying Your Configuration	23
Verifying Connectivity	23
Using Operational Commands	24
Related Topics	25

Chapter 2	Unidirectional Links	27
	Overview of Unidirectional Links	27
	Configurable Options	28
	Logical Interfaces	28
	Alarm Reporting	28
	Operational State	28
	Statistics	28
	System Requirements	29
	Configuring and Verifying Unidirectional Links	29
	Configuring and Verifying a Simple Example	29
	Configuring and Verifying a More Complex Example	31
	Related Topics	35

Part 2 **Voice Network Solutions**

Chapter 3	Overview of the Voice Solution	39
	The Voice Solution in a Next-Generation Network	39
	Terms and Abbreviations	40
	Voice Solution Architecture	41
	Packet Gateway Controller	41
	Packet Gateway on the JUNOS Routing Platform	42
	PGCP	42
	Voice Solution Topology with Multiple VPGs and PGCs	42
	Sample Network	44
	Controlling Voice Flows with Gates	44
	Gate Addressing	44
	Opening, Closing, and Modifying Gates	45
	Identifying Gates	45
	H.248 Building Blocks	45
	Terminations	46
	Contexts	46
	Streams	46
	Using Virtual Interfaces with the Packet Gateway	46
	Twice NAT for VoIP Traffic	47
	Providing Quality of Service for VoIP Traffic	47
	Providing Rate-Limiting for VoIP Traffic	47
	How the Rate-Limiting Feature Works	48
	Viewing Rate-Limiting Statistics	48
	Providing Security for PGCP Connections	48

Part 3 **Index**

Index	51
-------------	----

List of Figures

- Figure 1: Basic Video Network Topology6
- Figure 2: Basic IPTV Network Model7
- Figure 3: DSLAM Without IGMP Flow Recognition8
- Figure 4: DSLAM with IGMP Flow Recognition9
- Figure 5: IGMP Snooping10
- Figure 6: IGMP Proxy10
- Figure 7: IPTV Network (Access Side)17
- Figure 8: IPTV Network (Metro and Core Side)20
- Figure 9: Unidirectional Link Behavior27
- Figure 10: JUNOS Routing Platforms in the ETSI-TISPAN Architecture40
- Figure 11: Voice Solution Architecture41
- Figure 12: Topology with Multiple VPGs and PGCs43
- Figure 13: Active and Standby PGCs43
- Figure 14: Sample Voice Network44
- Figure 15: Unidirectional Gate44
- Figure 16: Addressing of Gate Pairs45
- Figure 17: Context, Termination, and Stream46
- Figure 18: Translation of Gate Addressing47

List of Tables

Table 1: Notice Icons	xiv
Table 2: Text and Syntax Conventions	xv
Table 3: Technical Documentation for Supported Routing Platforms	xvi
Table 4: JUNOS Software Network Operations Guides	xx
Table 5: Additional Books Available Through http://www.juniper.net/books	xxi
Table 6: Operational Commands for Network Verification	24
Table 7: Terms and Abbreviations	40

About This Guide

This preface provides the following guidelines for using the *JUNOS™ Software Multiplay Solutions Guide*:

- Objectives on page xiii
- Audience on page xiii
- Supported Routing Platforms on page xiv
- Using the Indexes on page xiv
- Documentation Conventions on page xiv
- List of Technical Publications on page xvi
- Documentation Feedback on page xxi
- Requesting Support on page xxii

Objectives

This guide describes how you can deploy IPTV and voice over IP (VoIP) services in your network.



NOTE: This guide documents Release 8.5 of the JUNOS software. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at <http://www.juniper.net/>.

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M-series, MX-series, T-series, or J-series routing platform.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Routing Platforms

For the features described in this manual, the JUNOS software currently supports the following routing platforms:

- J-series
- M-series
- MX-series
- T-series

Using the Indexes

This reference contains a standard index with topic entries.

Documentation Conventions

Table 1 on page xiv defines notice icons used in this guide.

Table 1: Notice Icons



Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.

Table 2 on page xv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> ■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> ■ A policy <i>term</i> is a named structure that defines match conditions and actions. ■ <i>JUNOS System Basics Configuration Guide</i> ■ RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> ■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

List of Technical Publications

Table 3 on page xvi lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 4 on page xx lists the books included in the *Network Operations Guide* series.

Table 5 on page xxi lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 3: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.

Table 3: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>High Availability</i>	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop routing (NSR) and graceful Routing Engine switchover (GRES).
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Multiplay Solutions</i>	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.

Table 3: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.

Table 3: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
J-series Routing Platform Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the Getting Started Guide for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.

Table 3: Technical Documentation for Supported Routing Platforms (*continued*)

Book	Description
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 4: JUNOS Software Network Operations Guides

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
<i>MPLS Fast Reroute</i>	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

Table 5: Additional Books Available Through <http://www.juniper.net/books>

Book	Description
<i>Interdomain Multicast Routing</i>	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.
<i>JUNOS Cookbook</i>	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
<i>MPLS-Enabled Applications</i>	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
<i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i>	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.
<i>Routing Policy and Protocols for Multivendor IP Networks</i>	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
<i>The Complete IS-IS Protocol</i>	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

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

Requesting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Part 1

IPTV Network Solutions

- IPTV Video Application on page 3
- Unidirectional Links on page 27

Chapter 1

IPTV Video Application

Next-generation multiplay networks are voice, data, and video networks that support personalized media and interactive IPTV services along with communications services such as voice over IP (VoIP) and Internet data transmission. These services place extreme demands on network scalability, quality of service, security, and bandwidth resources. Juniper Networks software provides support for configuring various broadband video architectures in a multiplay network.

Although the overview in this chapter discusses more than one video network model, the example focuses on one specific video network architecture that incorporates a video services router running JUNOS software Release 8.3 or later. To understand this chapter, you should be familiar with Broadband Remote Access Server (B-RAS) operation on Juniper Networks routers, as well as standard IGMP configurations.

For more information about B-RAS configuration, see the *JUNOS Broadband Access Configuration Guide*. For more information about IGMP configuration, see the *JUNOS Multicast Routing Configuration Guide*. You can obtain both manuals at:

<http://www.juniper.net/techpubs/software/index.html>

This chapter covers the following topics:

- System Requirements on page 4
- Terms and Acronyms on page 4
- Overview and Topology on page 5
- Sample Configuration of an IPTV Network on page 13
- Configuring the Access Side of a Video Services Router Running JUNOS Software on page 17
- Configuring the Metro and Core Side of a Video Services Router Running JUNOS Software on page 20
- Configuring Router Redundancy on page 22
- Verifying Your Configuration on page 23
- Related Topics on page 25

System Requirements

To implement video services on a routing platform running JUNOS software, you must use the following software and hardware components:

- JUNOS Release 8.3 or later for next-generation broadband or video features
- Juniper Networks video services routers (for example, the MX960 router or any M-series router that supports the JUNOS Release 8.3 or later video services software package)

Terms and Acronyms

- **ASM (Any Source Multicast)**—A method of allowing a multicast receiver to listen to all traffic sent to a multicast group, regardless of its source.
- **BSR (broadband services router)**—A router used for subscriber management and edge routing.
- **IGMP (Internet Group Membership Protocol)**—A host to router signaling protocol for IPv4 used to support IP multicasting.
- **IS-IS (Intermediate System-to-Intermediate System)**—A link-state, interior gateway routing protocol for IP networks that uses the shortest-path-first (SPF) algorithm to determine routes.
- **LSP (label-switched path)**—The path traversed by a packet that is routed by MPLS. Some LSPs act as tunnels. LSPs are unidirectional, carrying traffic only in the downstream direction from an ingress node to an egress node.
- **MPLS (Multiprotocol Label Switching)**—A mechanism for engineering network traffic patterns that functions by assigning to network packets short labels that describe how to forward the packets through the network.
- **OIF (outgoing interface)**—An interface used by multicast functions within a router to determine which egress ports to use for forwarding multicast groups.
- **OSPF (Open Shortest Path First)**—A link-state IGP that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm).
- **PIM (Protocol Independent Multicast)**—A multicast routing protocol used for delivering multicast messages in a routed environment.
- **routing gateway**—A firewall, NAT router, or other routing device used as a customer premises equipment (CPE) terminator in the home, office, or local point of presence (POP).
- **SSM (single-source multicast)**—Routing method that allows a multicast receiver to detect only a specifically identified sender within a multicast group.
- **set-top box**—The end host or device used to receive IPTV video streams.
- **VOD (video on demand)**—A unicast streaming video offering by service providers that enables the reception of an isolated video session per user with rewind, pause, and similar VCR-like capabilities.
- **VSR (video services router)**—A router used in a video services network to route video streams between an access network and a metro or core network. The

VSR is any M-series or MX-series router that supports the video routing package provided with JUNOS software Release 8.3 or later.

Overview and Topology

As an emerging genre of service, Internet Protocol television (IPTV) networks compete with more traditional video service offerings. IPTV networks provide new revenue streams to higher-premium multiplay services, which encompass bundled voice, video, Internet, gaming, and other services.

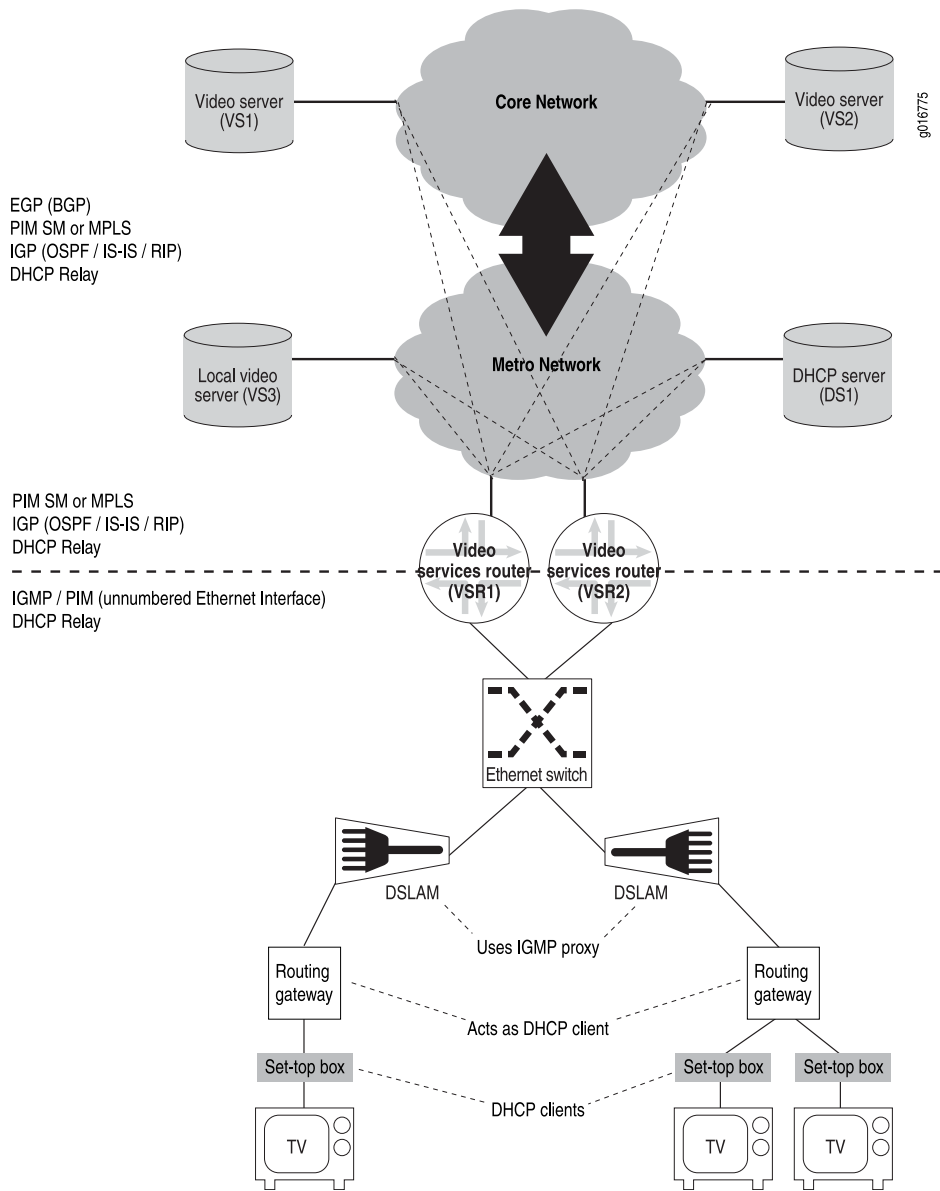
IPTV offers true integration of information, communications, and entertainment into personalized and interactive applications centered on familiar television-like services, including:

- Interactive entertainment services
- Broadcast services in standard and high-definition formats
- Video on demand (VOD)
- Digital video recording (DVR), including pausing and recording of broadcast TV, rewind, and fast-forward functionality
- Enhanced user services or interfaces such as an interactive programming guide and Mosaic interface, and converged features such as caller ID and message waiting

These new opportunities also present challenges to cost-effectively manage the delivery of performance-sensitive services over a service provider's IP infrastructure. Ensuring quality of service (QoS) for IPTV is essential, especially when the network is also carrying a wide array of other traffic. IPTV and similar latency-sensitive and jitter-sensitive services cannot be delivered at an acceptable quality of service simply through additional bandwidth. IPTV services must provide more efficient resource utilization while offering the best level of experience possible for subscribers.

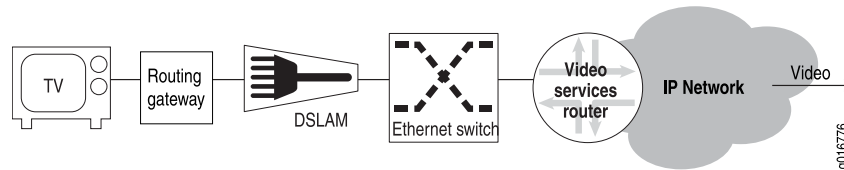
Figure 1 on page 6 shows a basic video network topology. The example in this chapter uses this topology. This network topology can be viewed as having two parts: an access side and a metro/core side. The demarcation of these two parts is at the video services router.

Figure 1: Basic Video Network Topology



Video Network Elements

The basic video (IPTV) network model, shown in Figure 2 on page 7, consists of up to five network elements.

Figure 2: Basic IPTV Network Model

These network elements are:

- Set-top box

At the subscriber site, a set-top box links the television to the external network. This device initiates channel change requests and responds to status inquiries.

- Routing gateway

The routing gateway, often close to the subscriber site or a part of the set-top box, aggregates traffic from multiple subscribers and may act upon requests from the set-top box.

- DSLAM

The DSLAM, like the routing gateway, aggregates traffic from multiple subscribers and may act on requests from the set-top box. The DSLAM often resides at a separate, centrally located office.

- Ethernet switch

Some networks can include an Ethernet switch or some other broadband services aggregator (BSA) to provide an additional layer of aggregation.

- Edge router

The edge router (typically a broadband services router [BSR] or video services router [VSR]) is the gateway into the backbone network. This device most often controls the multicast traffic to and channel requests from the set-top box.

IGMP and Video Networks

In a video (IPTV) network, broadcast television, pay-per-view (PPV), and video-on-demand (VOD) channels are all delivered by means of IP multicasting. Internet Group Management Protocol (IGMP) is the mechanism that controls the delivery of multicast traffic to subscribers on the network. This traffic is received and controlled by the subscriber's set-top box through multicast streams (referred to as channels). IGMP communicates with the upstream routing equipment to begin sending (join) or stop sending (leave) a channel.

Depending on the architecture that you choose for your network, the process of controlling channels occurs on a DSLAM, an aggregation switch, or an edge router.

IGMP Basics

Basic IGMP operation involves the following two devices:

- IGMP host (client)—Device that issues messages to join or leave a multicast group. This device also responds to queries from the multicast router. A set-top box is an example of an IGMP host.
- IGMP router (multicast router)—Device that responds to the join and leave messages to determine whether multicast groups should be forwarded from an interface. Periodic queries assist the router in recovering from any error conditions and verifying requests. The IGMP router receives multicast groups through the use of a multicast protocol, such as Protocol Independent Multicast (PIM), or through static flooding. An IGMP router is the termination point for any IGMP messages and therefore does not send any IGMP information to its upstream neighbors.

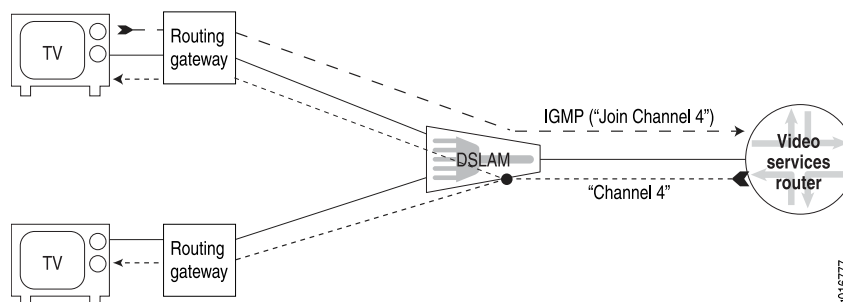
The IGMP protocol provides the following three basic functions for IP multicast networks:

- Join messages—Messages that indicate an IGMP host wants to receive information from (that is, become a member of) a multicast group.
- Leave messages—Messages that indicate an IGMP host no longer wants to receive information from a multicast group.
- Query messages—Messages from an IGMP router requesting information from a host. For example, if a set-top box is unplugged without first issuing a leave message, the IGMP router may query the host to determine what multicast groups the host belongs to.

IGMP and Intermediate Devices

In early IGMP networks, devices located between the IGMP client and the IGMP router did not detect IGMP flows. In Figure 3 on page 8, the top set-top box issues a request to view Channel 4, and the DSLAM forwards the request to the edge router. In response, the edge router begins forwarding the multicast group associated with Channel 4. However, if it does not detect IGMP flows, the intermediate device (in this case, the DSLAM) cannot appropriately forward the multicast traffic. By default, most switches broadcast incoming multicast traffic to all ports. In this case, the broadcast results in the bottom client receiving an unrequested channel.

Figure 3: DSLAM Without IGMP Flow Recognition

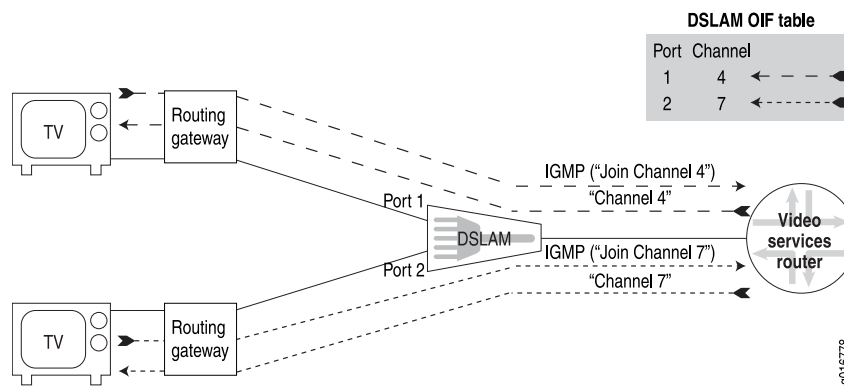


0016777

In these early networks, broadcasting of unrequested channels was not considered a problem, because multicast usage was low and the intermediate devices were typically LAN switches with lower interface and bandwidth costs. Now that IPTV requires higher bandwidth (often 4 Mbps per channel) and bandwidth costs more, it is crucial to ensure that IPTV channels are forwarded only to those subscribers currently viewing them.

To provide more intelligent control of bandwidth, DSLAMs and other intermediate devices now recognize IGMP flows. These devices examine incoming flows and build outgoing interface (OIF) tables. Figure 4 on page 9 shows a simple example of an outgoing interface table for the DSLAM. The outgoing interface table enables the DSLAM to appropriately forward each multicast group (or channel) from the correct port.

Figure 4: DSLAM with IGMP Flow Recognition



The intermediate device builds the outgoing interface table in one of two ways—IGMP snooping or IGMP proxy.

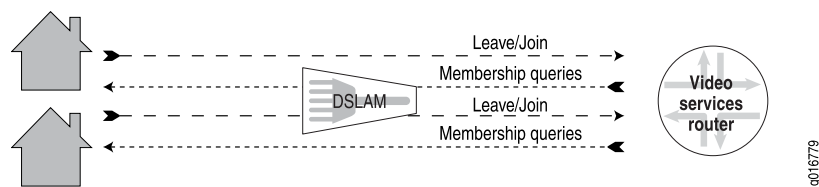


CAUTION: Some intermediate devices implement IGMP subsystems that use characteristics of both IGMP snooping and IGMP proxy. Most commonly, these devices might determine whether to forward IGMP packets (IGMP proxy) but do not modify the source IP address (IGMP snooping). We recommend that you avoid these nonstandard implementations.

IGMP Snooping

Figure 5 on page 10 illustrates IGMP snooping, in which an intermediate device (such as a DSLAM) transparently monitors IGMP traffic. The device adds interfaces to its outgoing interface table when it detects join request messages and removes interfaces from its outgoing interface table when it detects leave request messages. The snooping device also maintains state information for general *membership query maximum response time* timers if the IGMP client does not issue a leave message (for example, if an IPTV set-top box experiences a power outage).

Figure 5: IGMP Snooping



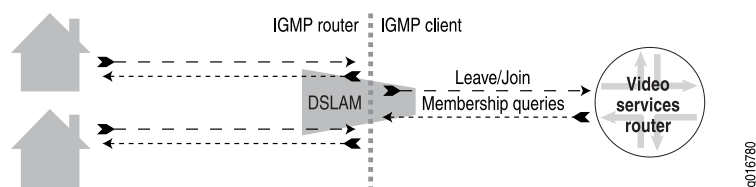
Because IGMP snooping is transparent, the snooping device typically does not participate in IGMP host messaging. The device only monitors transactions between clients and routers, forwarding IGMP packets upstream to the multicast router and determining when join or leave processing is required for a downstream host. One exception to this transparency occurs when the snooping device intercepts membership reports based on local filters to prevent the host from joining specific groups (that is, specific broadcast channels allocated to multicast groups that are blocked from being received by the set-top box).

The snooping device can receive multicast data in several ways within a broadband access network. The router might be configured to flood all multicast groups downstream to the snooping device. The upstream router might forward only groups based on IGMP membership reports that it receives from the IGMP hosts. The snooping agent might invoke an IGMP client process to source its own membership reports that it sends to the multicast router, and so on. However, these various options are beyond the scope of this document.

IGMP Proxy

Figure 6 on page 10 illustrates an IGMP proxy. An IGMP proxy performs functions of both an IGMP router and an IGMP client. When an IGMP host issues a join message, the IGMP proxy receives the message and adds the interface to its outgoing interface table for a specific multicast group. The proxy uses a general membership query timer and state to send general queries downstream to all multicast-enabled interfaces. When the IGMP proxy receives a leave message, the proxy issues a group-specific query. If no hosts respond to the query within a configured response time interval, the proxy removes the interface from the outgoing interface table.

Figure 6: IGMP Proxy



A device that functions as an IGMP proxy participates in every IGMP flow. This level of participation requires much more processing power and memory allocation from the DSLAM, but it can save upstream bandwidth.

Because a multicast router treats any IGMP proxy that it interacts with as an IGMP client, the multicast router tracks one device (the DSLAM) joining and leaving multicast

groups. As a result, the multicast router receives no information regarding subscribers on the other side of the IGMP proxy.

DHCP Relay and Video Services Routers

The Dynamic Host Configuration Protocol (DHCP) provides an automated mechanism for network devices to obtain configuration information and a lease for an IP address.

The most important configuration parameter carried by DHCP is the IP address. A computer must initially be assigned a specific IP address that is appropriate to the network to which the computer is attached and that is not assigned to any other computer on that network. If you move a computer to a new network, it must be assigned a new IP address for that new network. You can use DHCP to manage these assignments automatically.

DHCP carries other important configuration parameters, such as the subnet mask, default router, and DNS server.

The video services router must run DHCP relay to enable devices to obtain parameters from the DHCP server on the network. The DHCP relay feature relays a request from a remote client to a DHCP server for an IP address. When the router receives a DHCP request from an IP client, it forwards the request to the DHCP server and passes the response back to the IP client.

For more information about configuring DHCP relay, see the *JUNOS Policy Framework Configuration Guide*.

Video Networking and the Metro or Core Network

Video networks can incorporate various protocols used in the metro and core network. How you configure a metro or core network to transmit video streams depends on the type of network you have and the complexity of your application. All the protocols create multicast trees over which video streams can travel from one (or many) sources to a number of hosts.

What IP Routing Protocols to Use

When running video networks in an IP metro and core network, you must configure several protocols to function together. These protocols typically include the following protocol types:

- A multicast protocol to route multicast traffic
- An interior gateway protocol (IGP) to provide topological information to the multicast protocol
- An exterior gateway protocol (EGP) to route between different networks (depending on the complexity of your network)

What Multicast Protocol to Use

Video networks often use Protocol Independent Multicast sparse mode (PIM SM) when communicating beyond the access side of the network (that is, in the metro or core networks).

PIM is a family of multicast routing protocols that enable one-to-many and many-to-many distribution of data. The term *protocol-independent* means that PIM is not dependent on any particular unicast routing protocol for topology discovery. However, because it does not have its own method of topology discovery, PIM obtains routing information (such as dynamic endpoints) from other routing protocols, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS).

Instead of flooding packets throughout the network and then removing (or pruning) paths where no receivers exist, PIM SM uses the information it receives from the other routing protocols to construct a tree from each sender to the receivers in a multicast group.

What Interior Gateway Protocols to Use

PIM must use an IGP to obtain current topology information. The two protocols most often used by PIM to obtain topology information are OSPF and IS-IS. As IGPs, OSPF and IS-IS function within a single autonomous system (OSPF) or area (IS-IS).

Both OSPF and IS-IS are link-state routing protocols; they flood topology information throughout a network of routers within the autonomous system or area. After obtaining this information, each router independently builds a picture of the network topology. The routers can then forward packets or datagrams based on the best topological path through the network to the destination.

Using Exterior Gateway Protocols

Depending on the complexity and size of your network, you might need to configure an exterior gateway protocol (EGP). EGPs such as Border Gateway Protocol (BGP) exchange routing information between networks.

Using MPLS and Label-Switched Paths

Instead of using PIM SM to create multicast trees, you can use MPLS to control the paths that traffic takes to various destinations.

In the traditional Layer 3 forwarding paradigm, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. Each device analyzes the IP network layer header and then chooses the next hop based on the analysis and the information in the routing table.

In an MPLS environment, however, the packet header is analyzed only once, when the packet enters the MPLS network. After analyzing the packet header, the router assigns the packet to a stream that is identified by a label (a short, fixed-length value at the front of the packet). Downstream routers use these labels as lookup indexes for the label-forwarding table. The label-forwarding table stores forwarding information for each label.

A point-to-multipoint MPLS label-switched path (LSP) is an RSVP-signaled LSP with a single source and multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the ingress router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

Point-to-multipoint LSPs enable you to do the following:

- Use MPLS for point-to-multipoint data distribution similar to that provided by IP multicast.
- Add and remove branch LSPs from a main point-to-multipoint LSP without disrupting traffic. The unaffected parts of the point-to-multipoint LSP continue to function normally.
- Configure a node to be both a transit and an egress router for different branch LSPs of the same point-to-multipoint LSP.
- Use link protection on a point-to-multipoint LSP. Link protection can provide a bypass LSP for each of the branch LSPs that make up the point-to-multipoint LSP. If any of the primary paths fail, traffic can be switched quickly to the bypass.
- Configure subpaths either statically or dynamically.
- Specify graceful restart on point-to-multipoint LSPs.

For additional information about how to configure MPLS point-to-multipoint LSPs, see the *JUNOS MPLS Applications Configuration Guide*.

Redundancy and Failure Detection for Video Services Routers

Video networks require rapid failure detection and router redundancy to ensure minimal interruption of service. To provide a high level of failure detection and redundancy, you can employ PIM Bidirectional Forwarding Detection (BFD) for multicast traffic and Virtual Router Redundancy Protocol (VRRP) for unicast traffic in your video network.

Sample Configuration of an IPTV Network

This section provides a comprehensive sample configuration for the video services routers (VSR1 and VSR2) in the network topology shown in Figure 1 on page 6 and described in the following example sections.

Configuration for Router VSR1

```
[edit]
interfaces {
  ge-1/0/0 {
    unit 0 {
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
}
```



```

forwarding-options {
  dhcp-relay {
    server-group {
      DS1 {
        100.1.1.1;
      }
    }
    active-server-group DS1;
    group one {
      interface ge-1/0/0.0;
    }
  }
}
routing-options {
  static {
    route 1.1.1.1/32 {
      qualified-next-hop ge-1/0/0.0;
    }
  }
}

```

**Configuration for Router
VSR2**

```

[edit]
interfaces {
  ge-1/0/0 {
    unit 0 {
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
  ge-1/0/1 {
    unit 0 {
      family inet {
        address 10.1.1.2/24;
      }
    }
  }
  ge-1/0/1 {
    vlan-tagging;
    unit 1 {
      family inet {
        address 10.1.1.2/24 {
          vrrp-group 1 {
            virtual-address 10.1.1.99;
            priority 100;
            fast-interval 250;
          }
        }
      }
    }
  }
}
protocols {

```

```

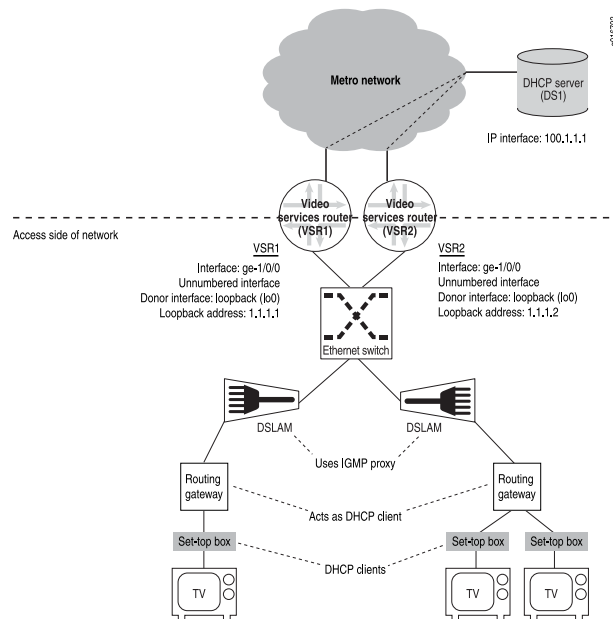
igmp {
  interface ge-1/0/0.0;
  promiscuous-mode;
  immediate-leave;
}
ospf {
  area 0 {
    interface ge-1/0/1;
  }
}
pim {
  rp {
    local {
      address 1.1.1.1;
    }
  }
  interface ge-1/0/0.0 {
    mode sparse;
    bfd-liveness-detection {
      minimum-interval 100;
    }
  }
  rp {
    local {
      address 1.1.1.1;
    }
  }
  interface ge-1/0/1.0 {
    mode sparse;
    bfd-liveness-detection {
      minimum-interval 100;
    }
  }
}
}
forwarding-options {
  dhcp-relay {
    server-group {
      DS1 {
        100.1.1.1;
      }
    }
    active-server-group DS1;
    group one {
      interface ge-1/0/0.0;
    }
  }
}
routing-options {
  static {
    route 1.1.1.2/32 {
      qualified-next-hop ge-1/0/0.0;
    }
  }
}
}

```

Configuring the Access Side of a Video Services Router Running JUNOS Software

The access (or customer) side of the JUNOS router operating in a video network uses IGMP and DHCP to manage video traffic to various clients. The interfaces on this side of the network use an unnumbered Ethernet configuration, as shown in Figure 7 on page 17.

Figure 7: IPTV Network (Access Side)



To implement video/IPTV applications on the access side of a video services router running JUNOS software, use the following procedures.



NOTE: To simplify this example, both video services routers (VSR1 and VSR2) use the same configuration except where otherwise specified.

1. Configure each access interface as an unnumbered Ethernet interface.

```
[edit]
interfaces {
  ge-1/0/0 {
    unit 0 {
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
}
```

2. Specify that the interface use promiscuous mode.



NOTE: You must specify that the IGMP interface use promiscuous mode if you define the unnumbered Ethernet donor interface as a loopback interface.

3. (Optional) Specify that the IGMP interface use immediate leave if you want the interface to do one of the following:
 - For IGMPv2: Immediately remove the group membership from the interface and suppress the sending of any group-specific queries for the multicast group.
 - For IGMPv3: Suppress the sending of group-and-source queries and rely on the JUNOS-supported host tracking mechanism to determine group membership removal.

```
[edit]
protocols {
  igmp {
    interface ge-1/0/0.0;
    promiscuous-mode;
    immediate-leave;
  }
}
```

4. Configure DHCP relay.

```
[edit]
forwarding-options {
  dhcp-relay {
    server-group {
      DS1 {
        100.1.1.1; # IP address of DHCP server (DS1)
      }
    }
  }
}
```

```

    }
  }
  active-server-group DS1;
  group one {
    interface ge-1/0/0.0; # interface to which DHCP clients send requests
  }
}

```

5. Configure PIM (required to configure PIM BFD).

```

[edit]
protocols {
  pim {
    rp {
      local {
        address 1.1.1.1;
      }
    }
    interface ge-1/0/0.0 {
      mode sparse;
    }
  }
}

```

6. Configure PIM BFD to enable rapid failover detection for the PIM interfaces.

```

[edit]
protocols {
  pim {
    interface ge-1/0/0.0 {
      bfd-liveness-detection {
        minimum-interval 100;
      }
    }
  }
}

```

7. Configure static routes over which each loopback interface can communicate with the other.

- a. Configure a static route on Router VSR1 to the loopback interface on Router VSR2.

```

[edit]
routing-options {
  static {
    route 1.1.1.2/32 {
      qualified-next-hop ge-1/0/0.0;
    }
  }
}

```

- b. Configure a static route on Router VSR2 to the loopback interface on Router VSR1.

```

[edit]

```

```

routing-options {
  static {
    route 1.1.1.1/32 {
      qualified-next-hop ge-1/0/0.0;
    }
  }
}

```

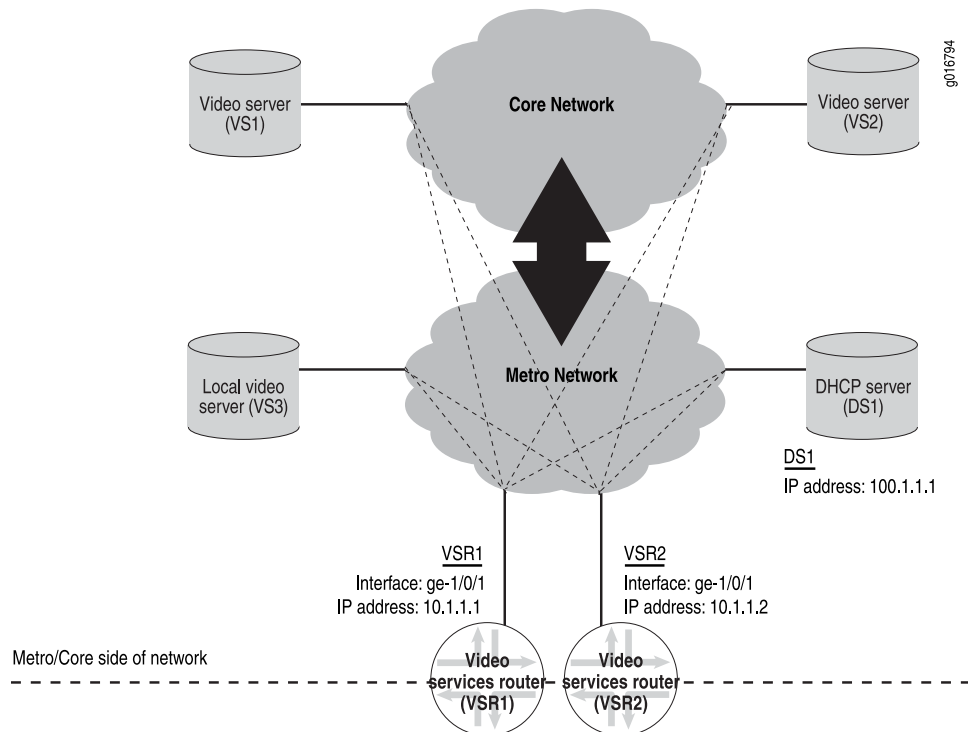


NOTE: You must also configure static routes for the DSLAM devices to communicate with the unnumbered interfaces that are using a loopback interface.

Configuring the Metro and Core Side of a Video Services Router Running JUNOS Software

The metro and core side of a router running JUNOS software and operating in a video network uses PIM SM or MPLS point-to-multipoint LSPs to manage video flows from various servers.

Figure 8: IPTV Network (Metro and Core Side)



When using PIM SM, you must also configure an Internal Gateway Protocol (IGP) to dynamically maintain a topology of the network that PIM SM can use.

To implement video applications on the metro and core side of a video services router running JUNOS software, use the following procedures:

1. Configure static IP addresses for the metro and core interface for both Router VSR1 and VSR2.
 - a. Configure a static IP address for Router VSR1.

```
[edit]
interfaces {
  ge-1/0/1 {
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
}
```

- b. Configure a static IP address for Router VSR2.

```
[edit]
interfaces {
  ge-1/0/1 {
    unit 0 {
      family inet {
        address 10.1.1.2/24;
      }
    }
  }
}
```



NOTE: You must define IP connectivity from the DHCP server (DS1) to the metro and core interface of Router VSR1 and VSR2.

2. Configure an internal gateway protocol (IGP). This example uses OSPF as the IGP for the network.

```
[edit]
protocols {
  ospf {
    area 0 {
      interface ge-1/0/1;
    }
  }
}
```

3. Configure PIM sparse mode (PIM SM).



NOTE: By default, IGMP is automatically enabled on all interfaces on which you configure PIM.

```
[edit]
protocols {
  pim {
    rp {
      local {
        address 1.1.1.1; # IP address of the PIM rendezvous point router
      }
    }
    interface ge-1/0/1.0 {
      mode sparse; # Define PIM SM on the metro and core interface
    }
  }
}
```

4. Configure PIM BFD to enable rapid failover detection for the PIM interfaces.

```
[edit]
protocols {
  pim {
    interface ge-1/0/1.0 {
      bfd-liveness-detection {
        minimum-interval 100;
      }
    }
  }
}
```

Configuring Router Redundancy

The bidirectional forwarding detection (BFD) protocol that you configured on each PIM interface uses control packets and shorter detection time limits to detect failures rapidly in a network for multicast traffic. However, to configure redundancy for unicast traffic in a video network (for example, for video-on-demand streams), you can use Virtual Router Redundancy Protocol (VRRP).

VRRP enables hosts on a LAN to use redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts.

At any time, one of the VRRP routing platforms is the master (active) and the others are backups. If the master fails, one of the backup routers becomes the new master router, thus always providing a virtual default routing platform and allowing traffic on the LAN to be routed without relying on a single routing platform.

To configure VRRP for each metro and core interface on the video services router, follow these steps.



NOTE: The VRRP groups must be the same for each router, and the VRRP priority setting must be lower for one of the routers.

1. Include the `vrrp-group` statement on the metro and core interface of Router VSR1.

```
[edit]
interfaces {
  ge-1/0/1 {
    vlan-tagging;
    unit 1 {
      family inet {
        address 10.1.1.1/24 {
          vrrp-group 1 {
            virtual-address 10.1.1.99;
            priority 200;
            fast-interval 250;
          }
        }
      }
    }
  }
}
```

2. Include the `vrrp-group` statement on the metro and core interface of Router VSR2.

```
[edit]
interfaces {
  ge-1/0/1 {
    vlan-tagging;
    unit 1 {
      family inet {
        address 10.1.1.2/24 {
          vrrp-group 1 {
            virtual-address 10.1.1.99;
            priority 100;
            fast-interval 250;
          }
        }
      }
    }
  }
}
```

Verifying Your Configuration

You can use several commands to verify that the IPTV network is functioning and to monitor its status.

Verifying Connectivity

When you configure your IPTV network, we recommend that you verify connectivity between routers (VSR1 and VSR2) and between each router and certain devices using the `ping` command.

The format for the `ping` command is as follows:

`ping host source source-address`

host—IP address of the device or interface to which you want to issue the `ping` command.

source source-address—IP address of the outgoing interface.

To verify connectivity:

- Issue the `ping` command from the access interface on each router to the loopback interface of the redundant router.
- Issue the `ping` command from each metro and core interface on each router to the metro and core interface on the redundant router.
- Issue the `ping` command from the loopback interface of each router to the DHCP server.

Using Operational Commands

You can use various operational commands to obtain information about the IPTV network and to verify that the network is operating properly. Table 6 on page 24 lists specific operational commands that can provide information about the IPTV network and the protocols that you configured on each video services router.

Table 6: Operational Commands for Network Verification

Operational Command	Purpose
<code>show dhcp relay binding</code>	The expected DHCP address bindings appear in the Dynamic Host Configuration Protocol (DHCP) client table.
<code>show dhcp relay statistics</code>	DHCP relay statistics are in line with expectations.
<code>show igmp group</code>	IGMP group membership is functioning as expected.
<code>show igmp interface</code>	<ul style="list-style-type: none"> ■ The status of each configured IGMP interface is operational (up). ■ The expected number of groups appears on each IGMP interface ■ Promiscuous mode is enabled (on) for IGMP unnumbered interfaces.
<code>show pim interfaces</code>	<ul style="list-style-type: none"> ■ The status of each PIM interface is operational (up). ■ Each interface is running sparse mode.
<code>show pim join</code>	<ul style="list-style-type: none"> ■ PIM group joins are occurring as expected. ■ Each join is receiving sparse mode entries.
<code>show pim neighbors</code>	<ul style="list-style-type: none"> ■ PIM is establishing neighbor adjacencies correctly.
<code>show pim neighbors detail</code>	<ul style="list-style-type: none"> ■ BFD is enabled.

Table 6: Operational Commands for Network Verification (continued)

Operational Command	Purpose
show pim rps	The PIM rendezvous point router is correct.
show pim statistics	PIM statistics are in line with expectations.

For additional information about these operational mode commands, see the *JUNOS Routing Protocols and Policies Command Reference*.

Related Topics

Because the concepts that constitute logical routers cut across the entire JUNOS software documentation set, you will find the following manuals to be useful references:

- For additional information about routing protocols, see the *JUNOS Routing Protocols Configuration Guide*.
- For additional information about interface configuration, see the *JUNOS Network Interfaces Configuration Guide*.
- For additional information about MPLS and related protocols, see the *JUNOS MPLS Applications Configuration Guide*.
- For additional information about multicast protocols, configuring flow maps and flow cache properties, and configuring bandwidth management, see the *JUNOS Multicast Protocols Configuration Guide*.
- For additional information about operational mode commands and output, see the *JUNOS Interfaces Command Reference*, the *JUNOS Routing Protocols and Policies Command Reference*, and the *JUNOS System Basics and Services Command Reference*.

Chapter 2

Unidirectional Links

- Overview of Unidirectional Links on page 27
- System Requirements on page 29
- Configuring and Verifying Unidirectional Links on page 29
- Related Topics on page 35

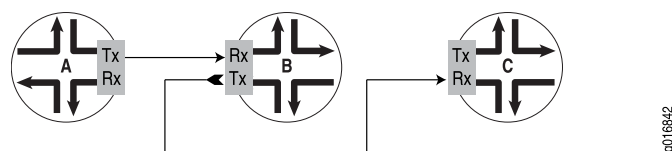
Overview of Unidirectional Links

Most of the traffic in a broadcast video cable network is directed downstream to the user. Conventional bidirectional links do not optimize bandwidth allocation to match the bandwidth requirements of this mostly one-way traffic flow. In addition, the bidirectional nature of ports requires a port to receive data from the same port that it transmits data to. This behavior quickly consumes port resources without using them effectively.

You can conserve port resources and address the bandwidth requirements by implementing unidirectional links in the network.

Physical interfaces operate in bidirectional mode by default, both transmitting and receiving traffic. When you configure unidirectional mode on the interface, two new physical interfaces are automatically created. One interface, designated by `-tx` in the interface name, can only transmit traffic. The other interface, designated by `-rx` in the interface name, can only receive traffic. The parent physical interface is still present, but you effectively see a port with two unidirectional links. Figure 9 on page 27 illustrates the unidirectional nature of the new interfaces.

Figure 9: Unidirectional Link Behavior



You can configure unidirectional mode on a per-port basis on the 10-Gigabit Ethernet interfaces of the 4-port 10-Gigabit Ethernet DPC on the MX960 platform only. You can configure both unidirectional and bidirectional ports on a single DPC.

Configurable Options

The transmit-only and receive-only interfaces created on a DPC port act independently. On the parent interface, you configure only the physical interface attributes common to both links. These attributes include clocking, framing, gigabit Ethernet options, and SONET options. On each of the unidirectional interfaces, you independently configure encapsulation (Ethernet only), MAC address, MTU size, address family (*inet* or *inet6*), and logical interfaces. VLAN tagging (untagged, single, stacked, or flexible) and VLAN IDs are also independently configurable on the receive-only and transmit-only interfaces. The full range of numbers for logical interfaces and VLAN IDs is available to both unidirectional interfaces.

To forward packets, you can configure only static ARP entries and static routes separately on each of the unidirectional interfaces. This configuration enables the transmit-only and receive-only interfaces to link to different ports on different routers. No other method of packet forwarding is currently supported.

The transmit-only and receive-only interfaces are removed when you delete unidirectional mode from the parent interface. The parent interface resumes operation as a normal, bidirectional interface.

Logical Interfaces

You cannot configure logical interfaces on the parent interface after you have configured unidirectional mode. However, you can configure logical interfaces on both the transmit-only interface and the receive-only interface.

Alarm Reporting

Alarms and defects are not reported for the transmit-only interface. Only local alarms and defects are reported for the receive-only interface. This behavior enables the use of SONET in a WAN-PHY configuration. SONET alarms, defects, and performance monitoring require bidirectional communication between sender and receiver. By accepting only local defects and alarms, the receiver interfaces in such a configuration are decoupled from the senders.

Operational State

The transmit-only link on a unidirectional port is always operationally up. Operational state is not influenced by the state of the receive-only link on that port.

Operational state of the receive-only link on a unidirectional port is independent of the state of the transmit-only link on that port. Link state for a receive-only link is determined only by the status of locally detected faults on the that link. Change in the state of the receive-only link can trigger traps, flap messages, and alarms.

Statistics

Statistics are reported differently for each of the three interfaces.

- Parent physical interface: No logical interfaces can be configured on the parent interface when it is in unidirectional mode. Therefore all traffic statistics for this

interface are reported as zero. All port-level statistics are reported on the parent physical interface rather than the rx or tx physical interfaces.

- Transmit-only physical interface: All transmit traffic statistics are reported for this interface. All receive (input) statistics are reported as zero. Also shown here are statistics for any logical interfaces configured on the transmit-only interface.
- Receive-only physical interface: All receive traffic statistics are reported for this interface. All transmit (output) statistics are reported as zero. Also shown here are statistics for any logical interfaces configured on the receive-only interface.

System Requirements

To implement unidirectional links, you must use the following hardware and software components:

- JUNOS Release 8.5 or later for configuring unidirectional mode
- One or more MX960 routers
- One or more 4-port 10-Gigabit Ethernet DPCs installed in each MX960 router

Configuring and Verifying Unidirectional Links

This section contains two examples and commands that you can use to configure and verify unidirectional links:

- [Configuring and Verifying a Simple Example on page 29](#)
- [Configuring and Verifying a More Complex Example on page 31](#)

Configuring and Verifying a Simple Example

To configure unidirectional mode using default settings on 10-Gigabit Ethernet interface xe-5/1/0 and confirm the configuration:

```
[edit]
interfaces xe-5/1/0 {
  unidirectional;
}

[edit]
user@host show interfaces
xe-5/1/0 {
  unidirectional;
}
```

The transmit-only and receive-only interfaces are created as soon as you commit the configuration. The following `show` command is one way to verify creation of these new interfaces:

```
user@host run show interfaces xe-5/1/0* terse
```

Interface	Admin	Link Proto	Local	Remote
xe-5/1/0	up	down		
xe-5/1/0-rx	up	down		
xe-5/1/0-tx	up	up		

The two unidirectional physical interfaces, xe-5/1/0-rx and xe-5/1/0-tx, are now present. In this example, no fiber-optic cables are connected to the port; consequently the xe-5/1/0 and xe-5/1/0-rx link states are down. In contrast, xe-5/1/0 is in the up state, because the transmit-only link is always up.

The following sample output provides more information about each of the interfaces. Unidirectional mode has been enabled on xe-5/1/0, the transmit-only and receive-only interfaces are present, and the link state matches expectations for no fiber-optic cables connected to the physical port.

```

user@host run show interfaces xe-5/1/0*
Physical interface: xe-5/1/0, Enabled, Physical link is Down
  Interface index: 318, SNMP ifIndex: 118
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Enabled, Loopback: None, Source filtering: Disabled,
  Flow control: Enabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 8 supported, 8 maximum usable queues
  Current address: 00:05:85:75:8b:62, Hardware address: 00:05:85:75:8b:62
  Last flapped  : 2007-08-10 11:45:29 PDT (01:39:47 ago)
  Active alarms : LINK
  Active defects: LINK
  PCS statistics
    Bit errors           Seconds
    Errored blocks      0
                        0

Physical interface: xe-5/1/0-rx, Enabled, Physical link is Down
  Interface index: 153, SNMP ifIndex: 129
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Rx-Only
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 8 supported, 8 maximum usable queues
  Current address: 00:05:85:75:8b:62, Hardware address: 00:05:85:75:8b:62
  Last flapped  : 2007-08-10 11:46:29 PDT (01:38:47 ago)
  Input rate    : 0 bps (0 pps)
  Output rate   : 0 bps (0 pps)
  Active alarms : LINK
  Active defects: LINK
  PCS statistics
    Bit errors           Seconds
    Errored blocks      0
                        0

Physical interface: xe-5/1/0-tx, Enabled, Physical link is Up
  Interface index: 158, SNMP ifIndex: 130
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Tx-Only
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 8 supported, 8 maximum usable queues

```

```

Current address: 00:05:85:75:8b:62, Hardware address: 00:05:85:75:8b:62
Last flapped   : 2007-08-10 11:46:29 PDT (01:38:47 ago)
Input rate    : 0 bps (0 pps)
Output rate   : 0 bps (0 pps)

```

Configuring and Verifying a More Complex Example

The following example makes the following changes from a default configuration:

- Sets framing mode to WAN-PHY on the parent interface, and consequently on the unidirectional interfaces as well.
- Configures VLAN IDs, VLAN tagging for single VLAN, and IP addresses on both unidirectional interfaces.
- Sets a nondefault MAC address on the receive-only interface.
- Configures a static ARP entry on the transmit-only interface. The entry contains a MAC address that is put into the Ethernet header destination address field of transmitted frames.

CLI Quick Configuration To quickly configure the example described, copy the following commands and paste them into the router terminal window:

```

[edit]
set interfaces xe-5/1/0 framing wan-phy
set interfaces xe-5/1/0 unidirectional
set interfaces xe-5/1/0-rx mac 00:12:34:56:78:90
set interfaces xe-5/1/0-rx vlan-tagging unit 102 vlan-id 102 family inet address
  10.1.102.2/24
set interfaces xe-5/1/0-tx vlan-tagging unit 201 vlan-id 201 family inet address
  10.2.201.2/24 arp 10.2.201.3 mac 00:ab:cd:cd:ab:cd
set routing-options static route 10.33.1.1/32 next-hop 10.2.201.3

```

Configuration Results Check the results of the configuration:

```

[edit]
user@host show interfaces
xe-5/1/0-rx {
  vlan-tagging;
  mac 00:12:34:56:78:90;
  unit 102 {
    vlan-id 102;
    family inet {
      address 10.10.102.2/24;
    }
  }
}
xe-5/1/0-tx {
  vlan-tagging;
  unit 201 {
    vlan-id 201;
    family inet {
      address 10.2.201.2/24 {
        arp 10.2.201.3 mac 00:ab:cd:cd:ab:cd;
      }
    }
  }
}

```

```

    }
  }
}
xe-5/1/0 {
  framing {
    wan-phy;
  }
  unidirectional;
}

```

Detailed Interface Information

To display terse details about the interfaces:

```

user@host run show interfaces xe-5/1/0* terse
Interface      Admin Link Proto  Local      Remote
xe-5/0/0       up    up
xe-5/0/0-rx   up    up
xe-5/0/0-rx.102 up    up    inet    1.1.102.2/24
                                     multiservice
xe-5/0/0-rx.32767 up    up    multiservice
xe-5/0/0-tx   up    up
xe-5/0/0-tx.201 up    up    inet    2.2.201.2/24
                                     multiservice
xe-5/0/0-tx.32767 up    up    multiservice

```

The additional logical interfaces for the unidirectional links result from the unit and VLAN tagging configuration.

To display more information about the interfaces:

```

user@host run show interfaces xe-5/1/0*
Physical interface: xe-5/1/0, Enabled, Physical link is Down
  Interface index: 151, SNMP ifIndex: 116
  Link-level type: Ethernet, MTU: 1514, Clocking: Internal, WAN-PHY mode, Speed:
  OC192, Unidirectional: Enabled, Loopback: None,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 8 supported, 8 maximum usable queues
  Current address: 00:05:85:75:8b:39, Hardware address: 00:05:85:75:8b:39
  Last flapped  : 2007-08-10 08:50:40 PDT (00:05:00 ago)
  Active alarms : LOF, LINK
  Active defects: LOF, SEF, AIS-L, AIS-P, LINK
  PCS statistics
    Bit errors          Seconds
    Errored blocks     0

```

```

Physical interface: xe-5/1/0-rx, Enabled, Physical link is Down
  Interface index: 153, SNMP ifIndex: 114
  Link-level type: Ethernet, MTU: 1518, WAN-PHY mode, Speed: OC192, Unidirectional:
  Rx-Only
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 8 supported, 8 maximum usable queues
  Current address: 00:12:34:56:78:90, Hardware address: 00:05:85:75:8b:39
  Last flapped  : 2007-08-10 08:50:40 PDT (00:05:00 ago)
  Input rate    : 0 bps (0 pps)

```

```

Output rate      : 0 bps (0 pps)
Active alarms   : LOF, LINK
Active defects  : LOF, SEF, AIS-L, AIS-P, LINK
PCS statistics
  Bit errors      : 0
  Errored blocks  : 0
  Seconds
Logical interface xe-5/1/0-rx.102 (Index 70) (SNMP ifIndex 115)
  Flags: Device-Down SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.102 ] Encapsulation:
ENET2
  Input packets : 0
  Output packets: 0
  Protocol inet, MTU: 1500
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
      Destination: 10.1.102/24, Local: 10.1.102.2, Broadcast: 10.1.102.255
  Protocol multiservice, MTU: Unlimited
  Flags: None

Logical interface xe-5/1/0-rx.32767 (Index 71) (SNMP ifIndex 124)
  Flags: Device-Down SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation:
ENET2
  Input packets : 0
  Output packets: 0
  Protocol multiservice, MTU: Unlimited
  Flags: None

Physical interface: xe-5/1/0-tx, Enabled, Physical link is Up
  Interface index: 158, SNMP ifIndex: 125
  Link-level type: Ethernet, MTU: 1518, WAN-PHY mode, Speed: OC192, Unidirectional:
Tx-Only
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:05:85:75:8b:39, Hardware address: 00:05:85:75:8b:39
  Last flapped   : 2007-08-10 08:50:40 PDT (00:05:00 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

Logical interface xe-5/1/0-tx.201 (Index 72) (SNMP ifIndex 126)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.201 ] Encapsulation: ENET2
  Input packets : 0
  Output packets: 0
  Protocol inet, MTU: 1500
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.2.201/24, Local: 10.2.201.2, Broadcast: 10.2.201.255
  Protocol multiservice, MTU: Unlimited
  Flags: None

Logical interface xe-5/1/0-tx.32767 (Index 73) (SNMP ifIndex 127)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
  Input packets : 0
  Output packets: 0
  Protocol multiservice, MTU: Unlimited
  Flags: None

```

You can use the `show interfaces xe-5/1/0* extensive` command to display the most complete set of information about the interfaces. Alternatively, you can specify only `xe-5/1/0`, `xe-5/1/0-rx`, or `xe-5/1/0-tx` to show extensive information about just one interface.

The extensive output includes statistics for the interfaces. The following excerpts show the differences between the receive-only and transmit-only interfaces for statistics.

In the following output for a receive-only interface, input statistics are recorded, but all output statistics have a value of zero.

```

user@host show interfaces xe-7/0/0-rx extensive
user@host> show interfaces xe-7/0/0-rx extensive
Physical interface: xe-7/0/0-rx, Enabled, Physical link is Up
  Interface index: 174, SNMP ifIndex: 118, Generation: 175
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
Unidirectional: Rx-Only
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : None
CoS queues    : 8 supported, 8 maximum usable queues
Hold-times    : Up 0 ms, Down 0 ms
Current address: 00:05:85:73:e4:83, Hardware address: 00:05:85:73:e4:83
Last flapped  : 2007-06-01 09:08:22 PDT (3d 02:31 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :          322857456303482          9627496104 bps
  Output bytes  :                   0                0 bps
  Input packets:          328775413751          1225495 pps
  Output packets:                   0                0 pps
...

Filter statistics:
  Input packet count          328775015056
  Input packet rejects                1
  Input DA rejects              0
...

Logical interface xe-7/0/0-rx.0 (Index 72) (SNMP ifIndex 120) (Generation 138)

Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes   :          322857456303482
  Output bytes  :                   0
  Input packets:          328775413751
  Output packets:                   0
...

Transit statistics:
  Input bytes   :          322857456303482          9627496104 bps
  Output bytes  :                   0                0 bps
  Input packets:          328775413751          1225495 pps
  Output packets:                   0                0 pps
...

```

In the following output for a transmit-only interface, output statistics are recorded, but all input statistics have a value of zero.

```

user@host> show interfaces xe-7/0/0-tx extensive
Physical interface: xe-7/0/0-tx, Enabled, Physical link is Up

```

```

Interface index: 176, SNMP ifIndex: 137, Generation: 177
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
Unidirectional: Tx-Only
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : None
CoS queues    : 8 supported, 8 maximum usable queues
Hold-times    : Up 0 ms, Down 0 ms
Current address: 00:05:85:73:e4:83, Hardware address: 00:05:85:73:e4:83
Last flapped  : 2007-06-01 09:08:19 PDT (3d 02:31 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes   :                0                0 bps
Output bytes  :   322891152287160   9627472888 bps
Input packets :                0                0 pps
Output packets:   328809727380   1225492 pps

```

...

```

Filter statistics:
Output packet count      328810554250
Output packet pad count  0
Output packet error count 0

```

...

Logical interface xe-7/0/0-tx.0 (Index 73) (SNMP ifIndex 138) (Generation 139)

```

Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
Input bytes   :                0
Output bytes  :   322891152287160
Input packets :                0
Output packets:   328809727380

```

...

```

Transit statistics:
Input bytes   :                0                0 bps
Output bytes  :   322891152287160   9627472888 bps
Input packets :                0                0 pps
Output packets:   328809727380   1225492 pps

```

...

Related Topics

For more information about concepts associated with unidirectional links, see the following resource:

- RFC 3077, *A Link-Layer Tunneling Mechanism for Unidirectional Links*

Part 2

Voice Network Solutions

- Overview of the Voice Solution on page 39

Chapter 3

Overview of the Voice Solution

This chapter describes the Juniper Networks voice solution for JUNOS routing platforms. Topics include:

- The Voice Solution in a Next-Generation Network on page 39
- Voice Solution Architecture on page 41
- Voice Solution Topology with Multiple VPGs and PGCs on page 42
- Sample Network on page 44
- Controlling Voice Flows with Gates on page 44
- H.248 Building Blocks on page 45
- Using Virtual Interfaces with the Packet Gateway on page 46
- Twice NAT for VoIP Traffic on page 47
- Providing Quality of Service for VoIP Traffic on page 47
- Providing Rate-Limiting for VoIP Traffic on page 47
- Providing Security for PGCP Connections on page 48

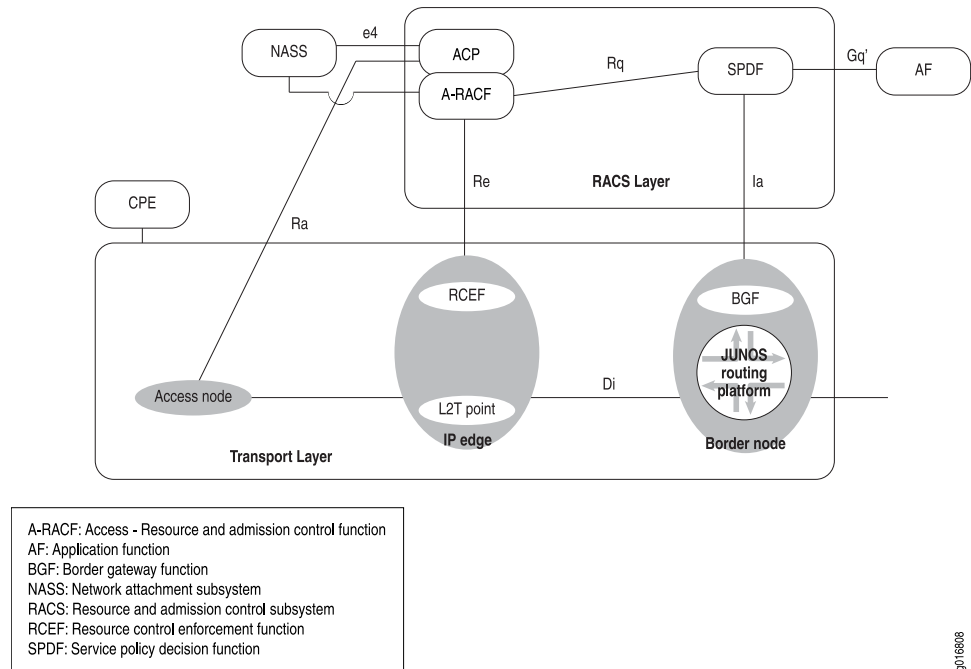
The Voice Solution in a Next-Generation Network

The voice solution provides a way for the router to integrate into a Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISpan)/IP multimedia subsystems (IMS) environment to provide voice over IP (VoIP) functionality. IMS is a flexible network architecture that allows providers to introduce multimedia services across both next-generation packet-switched and traditional circuit-switched networks. It uses open interfaces and functional components that can be assembled flexibly to support real-time interactive services and applications.

IMS provides a standards-based architecture that allows mobile carriers to migrate to next-generation networks that support applications that combine voice, video, and data functionality. The European Telecommunications Standards Institute (ETSI) created TISpan to extend IMS support to fixed-line carriers. This extension is commonly called fixed mobile convergence (FMC). IMS/FMC allows subscribers to access any network (wireless or fixed) from any device (computer, PDA, or cell phone) and to move seamlessly from one network to another.

The JUNOS routing platform acting as a packet gateway provides much of the border gateway function (BGF), as shown in the ETSI-TISPAN architecture in Figure 10 on page 40:

Figure 10: JUNOS Routing Platforms in the ETSI-TISPAN Architecture



9716806

Terms and Abbreviations

Table 7 on page 40 defines the terms and abbreviations used in this topic.

Table 7: Terms and Abbreviations

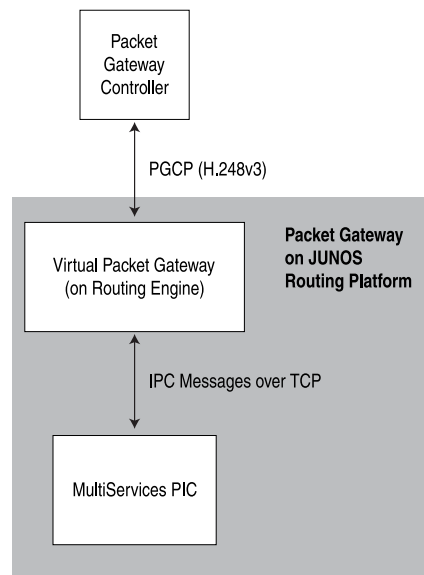
Term	Description
BGF	Border gateway function. The BGF resides in the transport layer and polices and enforces traffic flows based on instructions from the SPDF.
Context	An association between terminations.
Gate	Provides unidirectional forwarding of IP packets as directed by the PGC. A gate is sometimes called a pinhole.
Ia	A profile of the interface between an SPDF (the PGC) and the BGF (packet gateway).
I-BGF	Interconnect-BGF. The BGF between two peering partners. The packet gateway in the router provides much of the I-BGF function.
IMS	IP multimedia subsystem.
PG	Packet gateway. A virtual device on the router that provides media processing and control as directed by the PGC.

Table 7: Terms and Abbreviations (continued)

Term	Description
PGC	Packet gateway controller. The PGC is an external device that provides signal processing and directs the behavior of the PG. The PGC provides the service policy decision function (SPDF) shown in Figure 10 on page 40.
PGCP	Packet Gateway Control Protocol (PGCP). PGCP is an H.248 v3 protocol with Juniper Networks extensions. It provides management and signaling between the PG and the PGC.
SPDF	Service policy decision function. The SPDF controls the BGF. In the Juniper Networks voice solution, the PGC acts as the SPDF.
Stream	A bidirectional flow within a context.
Termination	A local source and sink of packets.

Voice Solution Architecture

As shown in Figure 11 on page 41, the two main components of the voice solution are the packet gateway controller (PGC) and the packet gateway (PG) feature on JUNOS routing platforms. The PGC and the PG communicate over the Packet Gateway Control Protocol (PGCP).

Figure 11: Voice Solution Architecture

g016801

Packet Gateway Controller

The PGC is an external device that controls the PG on the router. The PGC requests media services and resource allocation from the PG, and it uses those services and resources for VoIP call signaling setup. The PGC maintains awareness and control

over the network's transport resource using PGCP connections with all of the PGs in the network.

Packet Gateway on the JUNOS Routing Platform

The packet gateway feature on the router provides Interconnect-BGF transport services for VoIP sessions. The packet gateway feature consists of:

- Virtual packet gateways (VPGs)—A VPG consists of a packet gateway configuration on the Routing Engine. VPGs are controlled by a PGC. A VPG receives instructions from the PGC and instructs the MultiServices PIC how to treat voice traffic.

You can configure two VPGs in a router. Each VPG appears to the PGC as a separate network entity, and is connected to a PGC over its own PGCP connection. One VPG can connect to one PGC and one PIC at the same time.

- `pgcpd`—The packet gateway has a process called `pgcpd` running in the Routing Engine. The `pgcpd` process decodes PGCP messages that VPGs receive from the PGC and translates the PGCP messages to IPC messages.
- IPC—The VPGs and the MultiServices PIC communicate by exchanging Inter-Process Communication (IPC) messages over a TCP connection.
- MultiServices PIC—A MultiServices PIC controls voice traffic based on instructions it receives from the VPG.

PGCP

The PG and the PGC communicate over a Packet Gateway Control Protocol (PGCP) connection. PGCP is an H.248 v3 protocol with Juniper Networks extensions.

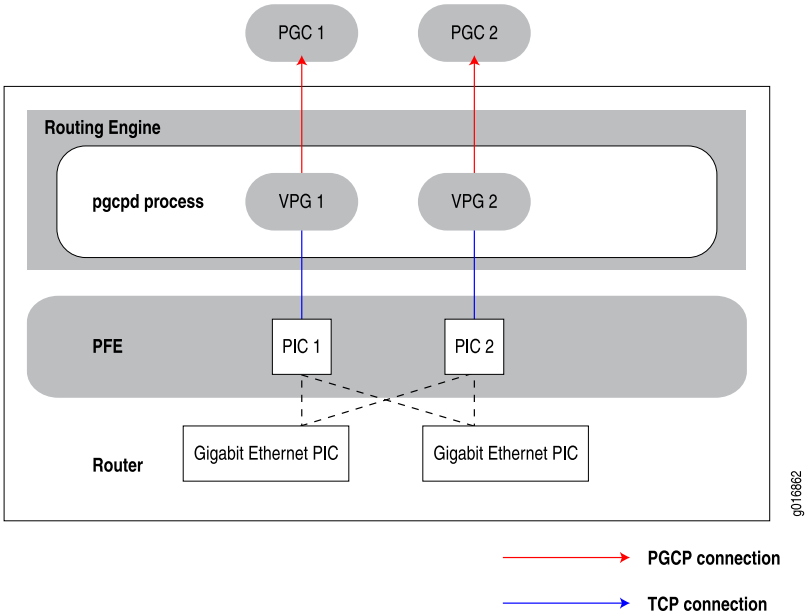
Voice Solution Topology with Multiple VPGs and PGCs

You can configure two VPGs in a router. Each VPG is connected to a PGC over its own PGCP connection. One VPG can connect to one PGC and one PIC at the same time.

Creating multiple VPGs allows you to deploy different policy and quality of service (QoS) characteristics in your network. It also allows you to scale your infrastructure by using multiple MultiServices PICs to control voice traffic.

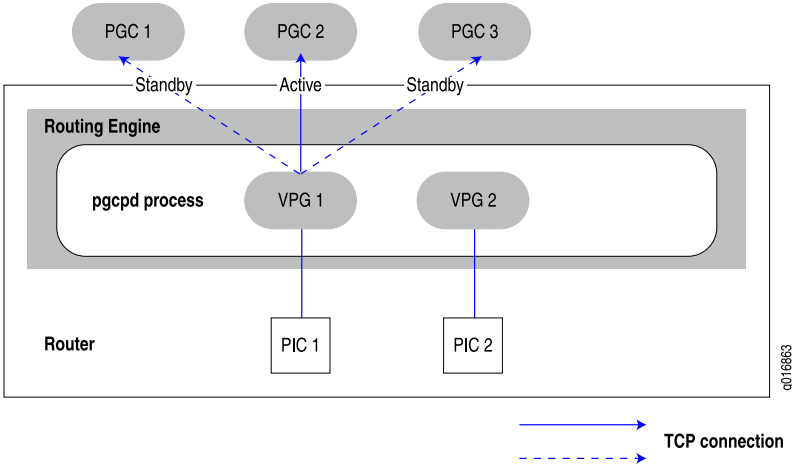
Figure 12 on page 43 shows a topology with multiple VPGs and PGCs. This topology allows one VPG and one MultiServices PIC to continue handling gate requests and forwarding packets on open gates even when the other PIC fails.

Figure 12: Topology with Multiple VPGs and PGCs



You can have multiple PGCs configured for one VPG. Only one PGC manages the VPG at a time. Other PGCs are on standby. When a VPG begins running on the router, it attempts to set up a connection to the first configured PGC. Each VPG can have one active PGC and one or more standby PGCs. In case of a PGC failure, the VPG can switch to another PGC. Figure 13 on page 43 shows an active and standby PGC connected to VPG 2.

Figure 13: Active and Standby PGCs

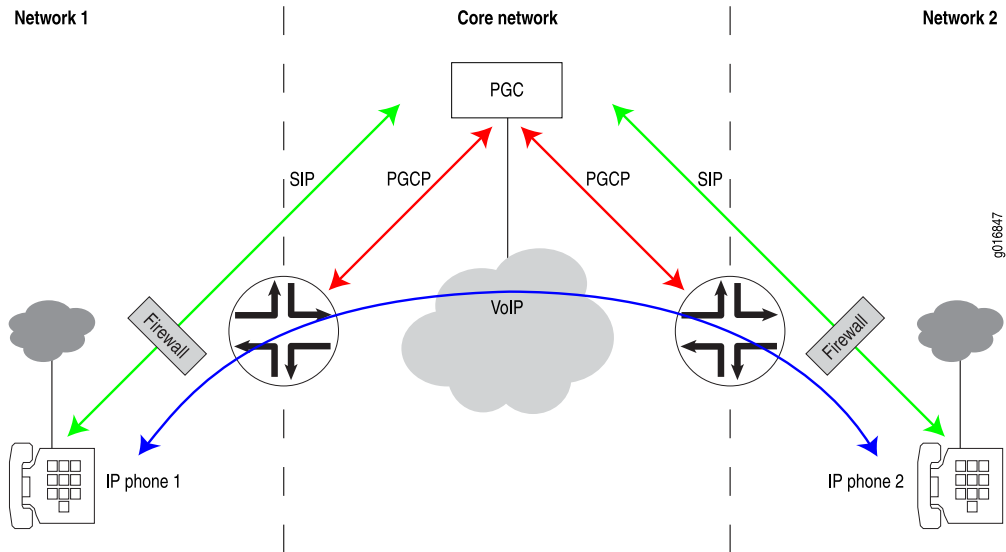


If the PGCP connection between the VPG and the PGC is lost, the VPG attempts to reconnect to the PGC. If the VPG cannot reconnect to the PGC, it traverses its list of PGCs until it successfully connects to one of the PGCs.

Sample Network

Figure 14 on page 44 shows a sample network that uses the voice solution.

Figure 14: Sample Voice Network

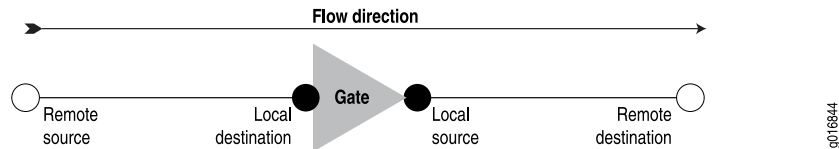


Controlling Voice Flows with Gates

The voice feature uses gates to control voice flows in the transport plane. Gates are created through signaling instructions that the PGC provides to the PG. Using the signaling instructions, the PG defines gates to allow, drop, or manipulate voice flows as they traverse the router.

Each gate provides a unidirectional voice flow. A pair of gates provides a bidirectional voice flow. Figure 15 on page 44 shows a unidirectional gate.

Figure 15: Unidirectional Gate



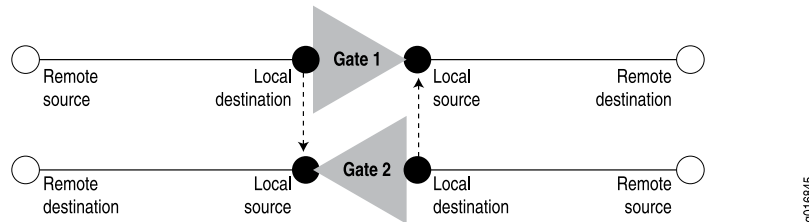
Gate Addressing

Gates are defined by their local source and destination addresses and their remote source and destination addresses.

Figure 16 on page 45 shows a gate pair, which represents a bidirectional voice flow. The local destination address of Gate 1 is equal to the local source address of Gate

2, and the local source address of Gate 1 is equal to the local destination address of Gate 2.

Figure 16: Addressing of Gate Pairs



Opening, Closing, and Modifying Gates

Based on information acquired through VoIP signaling, the PGC instructs the packet gateway through PGCP commands which gates to create and which actions to associate with them. Each gate can have many actions associated with it; for example, NAT, DSCP marking, and latching. The pgcpd process decodes PGCP commands that it receives from the PGC and uses IPC messages to instruct the PIC to create, delete, or modify gates and apply required actions to each gate.

The following IPC messages are exchanged between the pgcpd process and the PIC:

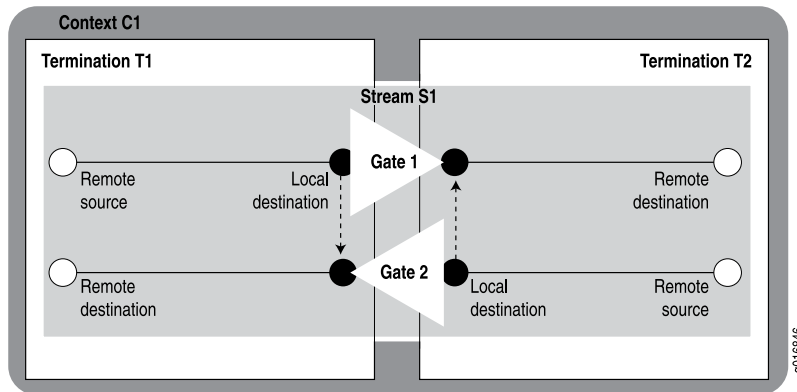
- Gate open request
- Gate close request
- Gate audit request
- Gate modify request
- Gate open reply
- Gate close reply
- Gate audit reply
- Gate modify reply
- Gate notification reply

Identifying Gates

When a gate is created, it is assigned an identifier. You can use this identifier with the PGCP `show` commands to monitor specific gates.

H.248 Building Blocks

The H.248 connection model uses contexts, terminations, and streams, which are logical entities that the PGC controls. In the router, the MultiServices PIC creates a context. The software then adds terminations to the context and adds streams to the terminations. Figure 17 on page 46 shows a context, termination, and stream.

Figure 17: Context, Termination, and Stream

Terminations

A termination can be a source and sink for media and control streams, and the parameters of the streams are encapsulated within the termination. A termination is characterized by properties that are grouped in a set of descriptors that are included in add, subtrace, modify, or audit commands. Terminations have unique identifiers (TerminationIDs) that the packet gateway assigns when it creates the termination.

Each termination is the source and destination of a gate. A termination exists only as long as a call. It is removed when the call is removed.

Contexts

A context is an association between a collection of terminations. The VPG instructs a MultiServices PIC to create a context for each voice session and each signaling session. Using instructions from the VPG, the PIC then applies policies such as DSCP, NAT, rate limiting, and inactivity timers to the gates within a context. If the VPG does not specify an existing context to which the termination is to be added, the PIC creates a new context.

Streams

A stream is one bidirectional flow within a context.

Using Virtual Interfaces with the Packet Gateway

The packet gateway and the PGC communicate through virtual interfaces. JUNOS interface names are not known or communicated to the PGC. You configure a virtual interface on the packet gateway, and this virtual interface is provided to the PGC. The virtual interface configuration includes the media service for the virtual interface, which contains the name of the NAT pool.

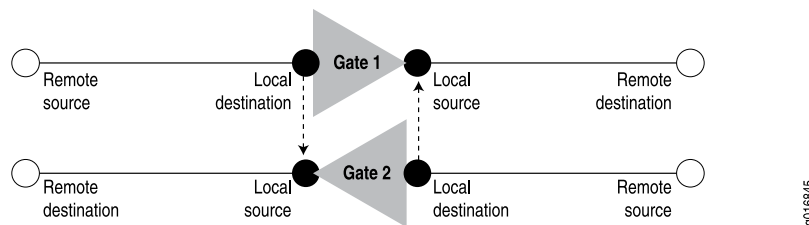
Included in the PGCP message exchange between the PGC and the VPG is a virtual interface identifier. This identifier instructs the packet gateway which media resources to use.

Twice NAT for VoIP Traffic

The packet gateway supports both network address translation (NAT) and network address port translation (NAPT). *Twice NAT* enables you to configure both source addresses and destination addresses that are translated as packets traverse the router. You can apply twice NAT for VoIP packets (signaling and media) as they traverse through the gates to achieve security between realms or service providers. To apply twice NAT, the pgcpd process instructs the PIC to allocate a specified number of NAT addresses and ports from a PGCP NAT pool on a per-gate basis. The pgcpd process specifies which NAT pool to use.

Figure 18 on page 47 shows two gates in a packet gateway.

Figure 18: Translation of Gate Addressing



After flows are created for gate 1, the gate connects the remote source to the local destination. The local source and local destination addresses reside on the router and must be uniquely specified. For gate 1, twice NAT enables the router to translate the IP address of the remote source to the local source, and the local destination to the remote destination.

To create the bidirectional flow, the same IP address is used for the local source in gate 2 and the local destination in gate 1. Likewise, the same IP address is used for the remote source in gate 1 and the remote destination in gate 2. You can configure application-level gateways (ALGs) for ICMP and traceroute in NAT flows; however, you cannot apply them to flows created by the packet gateway control function.

Providing Quality of Service for VoIP Traffic

To ensure optimized quality conditions for VoIP traffic, in gate open requests, the PGC can include a request for the packet gateway to mark voice traffic with various DSCP code points. The pgcpd process passes this information to the MultiServices PICs, which then apply these actions to the gate.

Providing Rate-Limiting for VoIP Traffic

Because PGCP traffic flows involve voice traffic, the flows require quality of service that:

- Provides the bandwidth that the flow requires.
- Ensures that flows do not consume more resources than they need.
- Regulates flows that are nonconforming and present vastly greater rates of traffic.

This quality of service is provided through a two-rate three-color policing functionality on the MultiServices PIC. This policer complies with *RFC 2698, A Two Rate Three Color Marker, September, 1999*. With the rate limiting capability, the MultiServices PIC can police flows to conform to:

- Committed Information Rate (CIR)
- Peak Information Rate (PIR)
- Committed Burst Size (CBS)
- Peak Burst Size (PBS)

How the Rate-Limiting Feature Works

You use rate limiting with PGCP gates. To enable rate limiting for a PGCP gate, you need to provide traffic management package (TMAN) parameters in the PGCP signaling commands that operate on gates. You configure these parameters on the PGC. These parameters are:

- Tman/sdr—Sustained data rate. This parameter provides the CIR.
- Tman/pdr—Peak data rate. This parameter provides the PIR.
- Tman/mbs—Maximum burst size. This parameter provides the burst size. Both the CBS and the PBS defined in RFC 2698 map to the maximum burst size.

The PGC sends the rate-limiting parameters to the packet gateway in PGCP gate open and gate modify signaling requests. When the MultiServices PIC receives these parameters, it marks the packets red, yellow, or green as specified in RFC 2698. A packet is marked red if it exceeds the PIR. A packet is marked yellow if it exceeds the CIR. A packet is marked green if it does not exceed the CIR. Packets that are marked red are dropped by the Multiservices PIC.

Viewing Rate-Limiting Statistics

To view rate-limiting statistics on a VPG, use the `show services pgcp gates gateway-name extensive` or the `show services pgcp gates gateway-name gate-id gate-id extensive operational mode` command.

Providing Security for PGCP Connections

If the underlying network layer does not support IPSec, you can use the interim authentication header (AH) scheme to provide security on the connection between the VPG and the PGC. The interim AH scheme defines an AH header with the H.248 protocol header. To use the interim AH scheme, configure the a security algorithm for the interim AH scheme in the VPG configuration.

Part 3

Index

- Index on page 51

Index

Symbols

#, comments in configuration statements.....	xv
(), in syntax descriptions.....	xv
< >, in syntax descriptions.....	xv
[], in configuration statements.....	xv
{ }, in configuration statements.....	xvi
(pipe), in syntax descriptions.....	xv

B

BGF (border gateway function)	
voice solution.....	40
border gateway function. <i>See</i> BGF	
braces, in configuration statements.....	xvi
brackets	
angle, in syntax descriptions.....	xv
square, in configuration statements.....	xv

C

comments, in configuration statements.....	xv
contexts.....	46
conventions	
text and syntax.....	xv
core network and video networking.....	11
curly braces, in configuration statements.....	xvi
customer support.....	xxii
contacting JTAC.....	xxii

D

DHCP	
video services router and.....	11
documentation set	
comments on.....	xxi
DSLAM outgoing interface table.....	9
DSLAM, in IPTV video network.....	7

E

edge router, in IPTV video network.....	7
Ethernet switches	
in IPTV video network.....	7

F

failure detection in video networks.....	13
font conventions.....	xv

G

gates, voice solution	
addressing.....	44
controlling voice flows.....	44
identifying.....	45
opening, closing, modifying.....	45

H

H.248 building blocks.....	45
contexts.....	46
streams.....	46
terminations.....	46

I

icons defined, notice.....	xiv
IGMP	
host (client).....	8
intermediate devices.....	8
router (multicast router).....	8
video networks and.....	7
IGMP proxy.....	10
IGMP snooping.....	9
Inter-Process Communication. <i>See</i> IPC	
IP routing protocols	
in IPTV metro and core network.....	11
IPC (Inter-Process Communication)	
voice solution.....	42
IPTV video application	
connectivity, verifying.....	23
IGMP and.....	7
network elements.....	6
network topology.....	6
operational commands.....	24
overview.....	5
sample configuration.....	13
system requirements.....	4
verifying operation.....	23

IPTV video networks
 verifying configuration.....23

J

join messages, IGMP.....8

L

Layer 3 VPNs
 multicast
 system requirements.....4
 leave messages, IGMP.....8
 LSPs
 in video networks.....12

M

manuals
 comments on.....xxi
 metro network and video networking.....11
 multicast
 Layer 3 VPNs
 system requirements.....4

N

notice icons defined.....xiv

O

operational mode commands
 for IPTV video network verification.....24

P

packet gateway
 voice solution.....42
 Packet Gateway Control Protocol (PGCP). *See* PGCP
 packet gateway controller (PGC). *See* PGC
 parentheses, in syntax descriptions.....xv
 PGC
 voice architecture.....41
 PGCP.....41
 pgcpd process
 voice solution.....42
 PIM SM
 in video networks.....12

Q

query messages, IGMP.....8

R

rate-limiting, voice traffic.....47

redundancy in video networks.....13
 routing gateway, in IPTV video network.....7

S

set-top box, in IPTV video network.....7
 streams.....46
 support, technical *See* technical support
 syntax conventions.....xv
 system requirements
 multicast over Layer 3 VPNs.....4

T

technical support
 contacting JTAC.....xxii
 terminations.....46
 twice NAT, voice traffic.....47

V

video networking
 metro or core network and.....11
 video services routers
 access side, configuring.....17
 metro and core side, configuring.....20
 redundancy, configuring.....8, 22
 virtual packet gateway. *See* VPG
 voice solution
 architecture.....41
 gates.....44
 addressing.....44
 identifying.....45
 opening, closing, modifying.....45
 H.248 building blocks.....45
 contexts.....46
 streams.....46
 terminations.....46
 overview.....39
 packet gateway.....42
 packet gateway controller.....41
 rate-limiting.....47
 sample network.....44
 topology with multiple VPGs and PGCs.....42
 twice NAT.....47
 VPG (virtual packet gateway)
 voice solution.....42
 multiple VPGs.....42
 VRRP
 on video services routers.....22