JUNOS® Software

Multiplay Solutions Guide

Release 9.6

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

Published: 2009-07-15

JUNOS® Software Multiplay Solutions Guide
Release 9.6

Writing: Mark Barnard, Justine Kangas, Sarah Lesway-Ball, Brian Wesley Simmons
Editing: Ben Mann
Illustration: Nathaniel Woodward, Mark Barnard
Cover Design: Edmonds Design

Revision History
July 2009—R1 JUNOS 9.6

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

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

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

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

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

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

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

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

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

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

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

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

Table of Contents

List of Figures

List of Tables

About This Guide

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

JUNOS Documentation and Release Notes

For a list of related JUNOS documentation, see http://www.juniper.net/techpubs/software/junos/.

If the information in the latest release notes differs from the information in the documentation, follow the *JUNOS Software Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using JUNOS Software and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using JUNOS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books.

Objectives

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

NOTE: For additional information about 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, EX Series, or J Series router or switch.

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:

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

Using the Indexes

This reference contains a standard index with topic entries.

Documentation Conventions

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

Table 1: Notice Icons

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

Table 2 on page xxv 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`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

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

Convention	Description	Examples
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. ■ The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**
Indention and braces (**{ }**)	Identify a level in the configuration hierarchy.	**[edit** **routing-options {** **static {** **route default {** **nexthop *address*;** **retain;** **}** **}** **}**
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	■ In the Logical Interfaces box, select **All Interfaces**. ■ To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols > Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. 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 (not required for Network Operations Guides [NOGs])

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1
IPTV Network Solutions

Chapter 1

IPTV Video Application

Next-generation multiplay networks are voice, data, and video networks that support personalized media and interactive IP television (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. JUNOS 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 Internet Group Management Protocol (IGMP) configurations.

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

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

This chapter covers the following topics:

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 Ethernet Services 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 (IGRP) 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 fowarding multicast groups.
- **OSPF (Open Shortest Path First)**—A link-state interior gateway protocol (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, Network Address Translation (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)**—A 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 router 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.

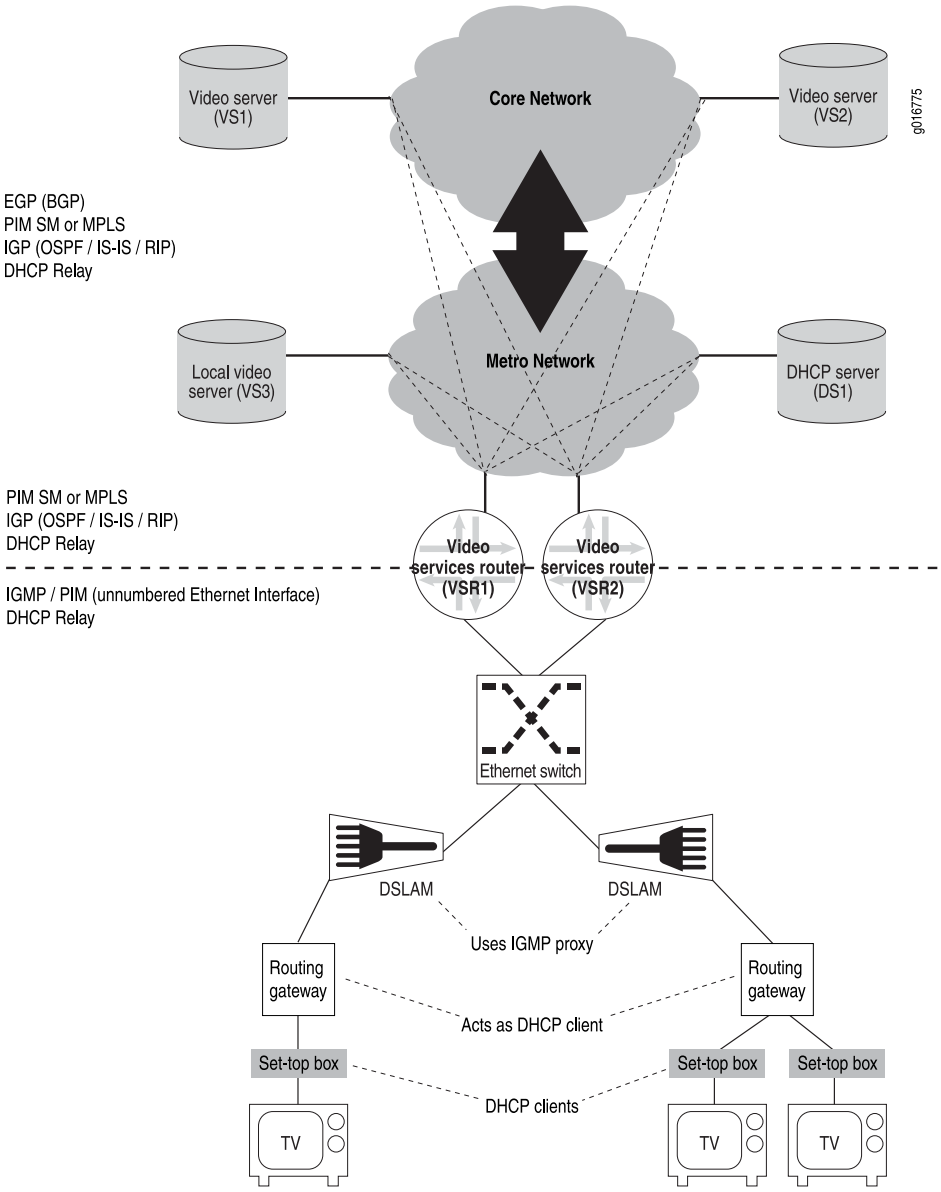
IPTV offers true integration of information, communications, and entertainment into personalized and interactive applications centered on familiar television-like services, including:

- 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.

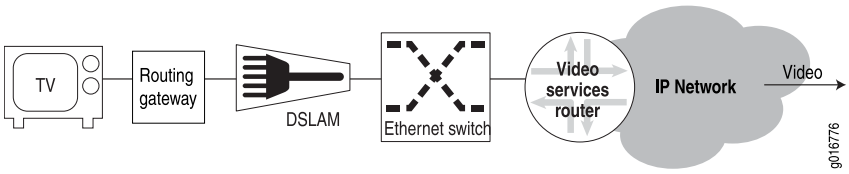
Figure 1: Basic Video Network Topology



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 digital subscriber line access multiplier (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 or not to forward multicast groups 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.

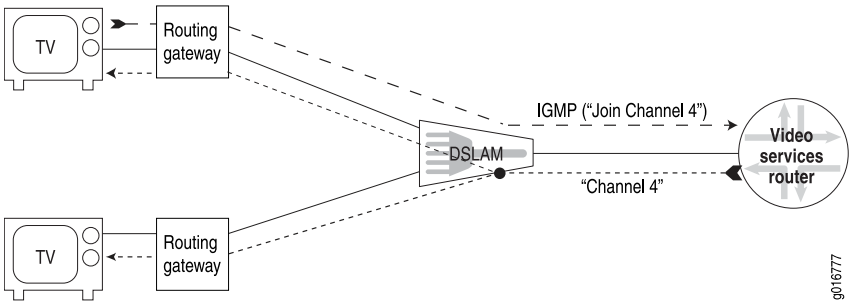
The IGMP protocol provides the following three basic functions for IP multicast networks:

- 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 9, 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.

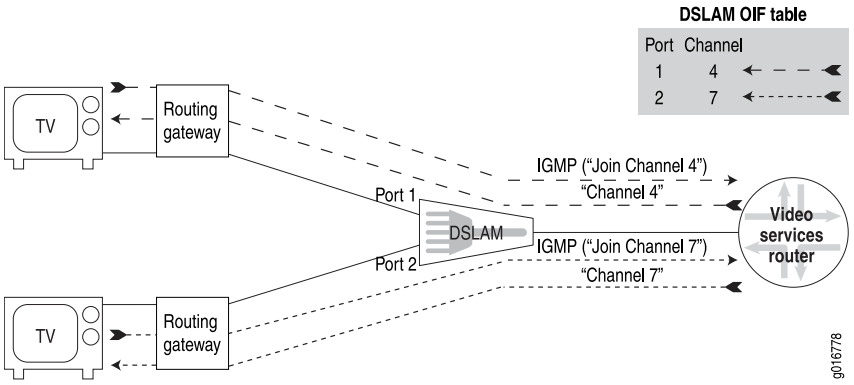
Figure 3: DSLAM Without IGMP Flow Recognition



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



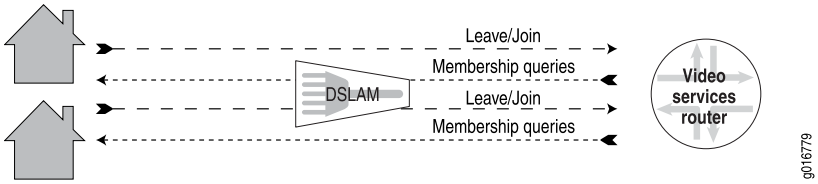
The intermediate device builds the outgoing interface table in one of two ways—IGMP snooping or IGMP proxy.

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



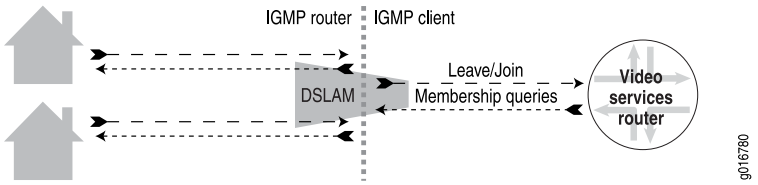
Because IGMP snooping is transparent, the snooping device typically does not participate in IGMP host messaging. The device only monitors transactions between clients and routers, forwarding IGMP packets upstream to the multicast router and determining when join or leave processing is required for a 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 11 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)

Multicast Protocols 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.

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.

Exterior Gateway Protocols to Use—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;
         }
      }
   }
   ge-1/0/1 {
      unit 0 {
         family inet {
            address 10.1.1.1/24;
         }
      }
      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;
               }
            }
         }
      }
   }
}
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 1.1.1.1/32 {
        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 {
```

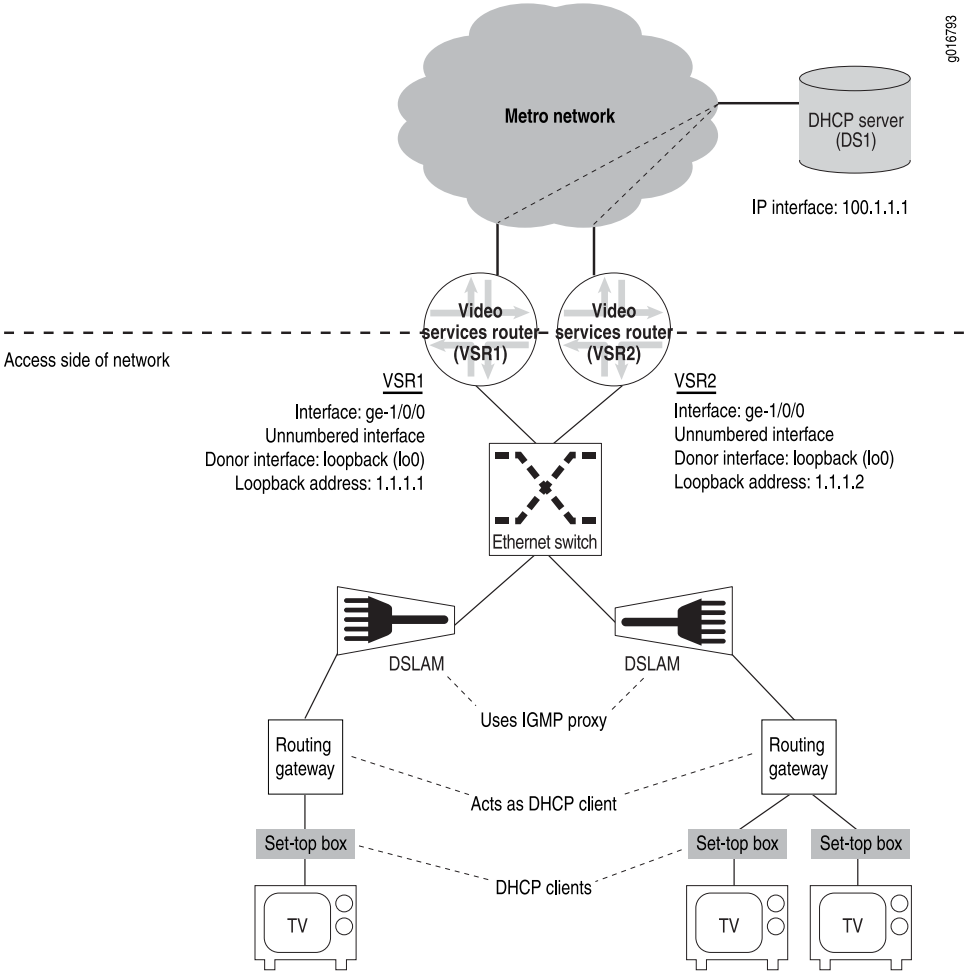
```
            address 10.1.1.2/24 {
               vrrp-group 1 {
                  virtual-address 10.1.1.99;
                  priority 100;
                  fast-interval 250;
               }
            }
         }
      }
   }
}
protocols {
   igmp {
      interface ge-1/0/0.0;
      promiscuous-mode;
      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 router running JUNOS Software and 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. 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 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]
```

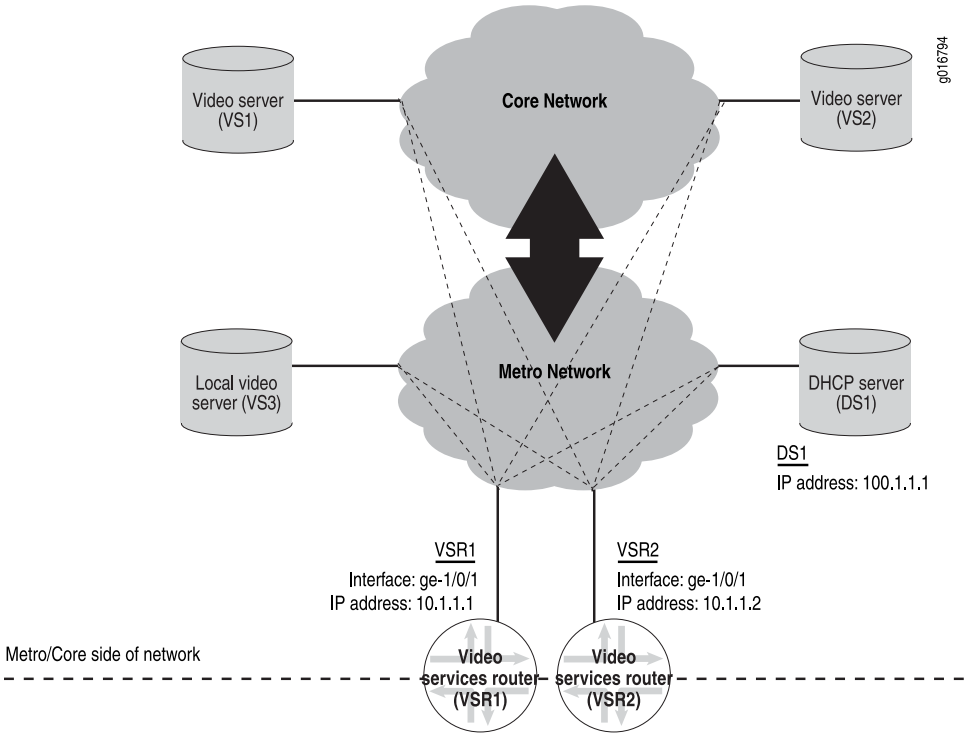
```
routing-options {
   static {
      route 1.1.1.1/32 {
         qualified-next-hop ge-1/0/0.0;
      }
   }
}
```

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 3 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 3: Operational Commands for Network Verification

Operational Command	Purpose
show dhcp relay binding	The expected DHCP address bindings appear in the Dynamic Host Configuration Protocol (DHCP) client table.
show dhcp relay statistics	DHCP relay statistics are in line with expectations.
show igmp group	IGMP group membership is functioning as expected.
show igmp interface	■ 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.
show pim interfaces	■ The status of each PIM interface is operational (up). ■ Each interface is running sparse mode.
show pim join	■ PIM group joins are occurring as expected. ■ Each join is receiving sparse mode entries.
show pim neighbors show pim neighbors detail	■ PIM is establishing neighbor adjacencies correctly. ■ BFD is enabled.

Table 3: 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, the following manuals can 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

This chapter describes unidirectional links and how to configure them. Topics include:

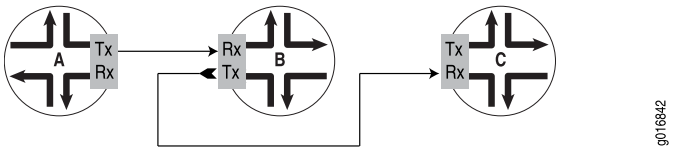
Overview of Unidirectional Links

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 link 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 link mode on a per-port basis on the 10-Gigabit Ethernet interfaces of the following hardware only:

- 4-port 10-Gigabit Ethernet DPC on the MX960 Ethernet Services Router
- IQ2 PIC and IQ2E PIC on the T Series Core Routers

You can configure both unidirectional and bidirectional ports on a single DPC or PIC.

Configurable Options

The transmit-only and receive-only interfaces created on a 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 be shared between both unidirectional interfaces. That is, the number configured on receive-only interfaces plus the total configured on the transmit-only interfaces cannot exceed the available range.

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 link 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 link 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 link 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 one of the following hardware and software combinations:

- MX Series router running JUNOS Release 8.5 or later, with one or more 4-port 10-Gigabit Ethernet DPC installed
- T Series router running JUNOS Software Release 9.5 or later, with one or more 10-Gigabit Ethernet IQ2 PIC or 10-Gigabit Ethernet IQ2E PIC installed

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 link 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 link 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                      Seconds
    Bit errors                             0
    Errored blocks                         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                      Seconds
    Bit errors                             0
    Errored blocks                         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

Display 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                      Seconds
    Bit errors                             0
    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                      Seconds
    Bit errors                             0
    Errored blocks                         0

  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
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
BGF VoIP Solution

Chapter 3

Overview of the BGF VoIP Solution

This chapter describes the Juniper Networks border gateway function (BGF) voice over IP (VoIP) solution. Topics include:

The BGF VoIP Solution in a Next-Generation Network Overview

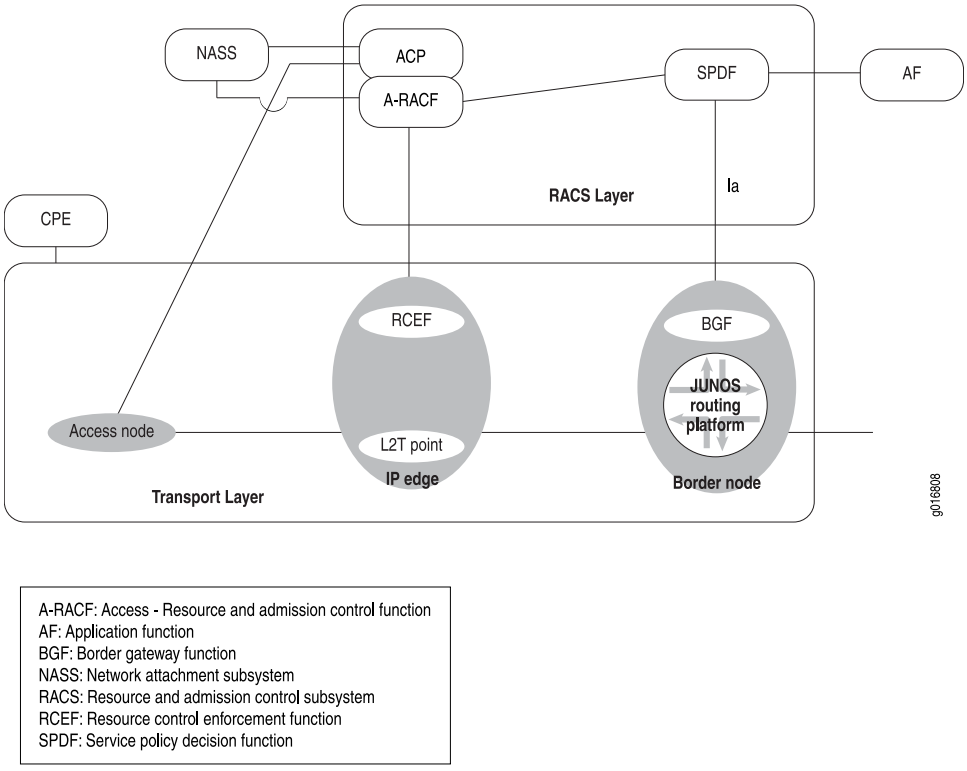
The BGF VoIP solution provides a way for the router to integrate into a Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN)/IP multimedia subsystems (IMS) environment to provide VoIP functionality. IMS is a flexible network architecture that allows providers 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 router provides the BGF role, as shown in the ETSI-TISPAN architecture in Figure 10 on page 40:

Figure 10: Routers Running JUNOS Software in the ETSI-TISPAN Architecture



A-RACF: Access - Resource and admission control function
AF: Application function
BGF: Border gateway function
NASS: Network attachment subsystem
RACS: Resource and admission control subsystem
RCEF: Resource control enforcement function
SPDF: Service policy decision function

BGF VoIP Solution Terms and Abbreviations

Table 4 on page 40 defines the terms and abbreviations used in this topic.

Table 4: Terms and Abbreviations

Term	Description
BGF	Border gateway function. Resides in the transport layer and polices and enforces traffic flows based on instructions from the SPDF. The router provides the BGF functionality.
Context	An association between terminations.
Gate	Unidirectional flow of IP packets as directed by the gateway controller. Sometimes called a pinhole.
Gateway Controller	In the BGF VoIP solution, an external device that provides signal processing and directs the behavior of the BGF. The gateway controller provides the service policy decision function (SPDF) shown in Figure 10 on page 40.
Ia	A profile of the interface between an SPDF (the gateway controller) and the BGF.

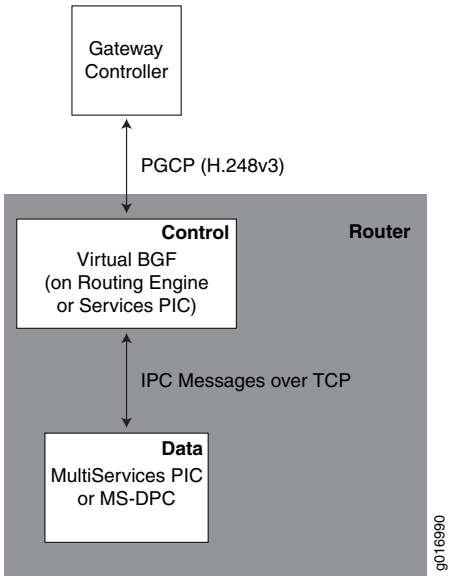
Table 4: Terms and Abbreviations *(continued)*

Term	Description
I-BGF	Interconnect-BGF. The BGF between two peering partners.
IMS	IP multimedia subsystem.
IPC	The virtual BGFs and the MultiServices PIC or MultiServices Dense Port Concentrator (MS-DPC) communicate by exchanging Inter-Process Communication (IPC) messages over a TCP connection; this is internal (intra-chassis) communication.
PGCP	Packet Gateway Control Protocol (PGCP). An H.248 v3 protocol with Juniper Networks extensions. It provides management and signaling between the BGF and an external gateway controller.
pgcpd	A process that decodes H.248 messages that BGFs receive from external gateway controllers and translates the H.248 messages to IPC messages. You can configure the pgcpd process to run in the Routing Engine or on a MultiServices PIC.
SPDF	Service policy decision function. Controls the BGF. In the Juniper Networks BGF VoIP solution, an external gateway controller acts as the SPDF.
Stream	A bidirectional flow within a context.
Termination	A local source and sink of packets.
Virtual BGF	A virtual device on the router that provides media processing and control as directed by the gateway controller.

BGF VoIP Solution Architecture

As shown in Figure 11 on page 42, the two main components of the voice solution are the BGF and the gateway controller. The BGF and the gateway controller communicate over the Packet Gateway Control Protocol (PGCP).

Figure 11: BGF Voice Solution Architecture



Gateway Controller

In the BGF VoIP solution, the gateway controller is an external device that controls the BGF on the router. The gateway controller requests media services and resource allocation from the BGF, and it uses those services and resources for VoIP call signaling setup. The gateway controller maintains awareness and control over the network's transport resource using PGCP connections with all of the BGFs in the network.

BGF

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

- Virtual BGFs.
- pgcpd process that controls the virtual BGFs.
- A data PIC that controls voice traffic based on instructions it receives from the virtual BGFs. You can use MultiServices PICs or MS-DPCs as the data PIC.
- An optional control PIC. You can run the virtual BGFs with the pgcpd process on either the Routing Engine or on a PIC. If you run your virtual BGFs on a control PIC, you can use MultiServices PICs or MS-DPCs. The MultiServices 500 PIC is not supported as the control PIC.

You can run up to eight concurrent virtual BGFs in a router. The eight virtual BGFs can run on the same control services PIC. All virtual BGFs on a router must run in either the Routing Engine or on services PICs. You cannot run some virtual BGFs on the Routing Engine and some on services PICs.

PGCP

The BGF and the gateway controller communicate over a Packet Gateway Control Protocol (PGCP) connection. PGCP is an H.248 v3 protocol with Juniper Networks extensions. PGCP complies with *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005* and with *H.248 Profile for controlling Border Gateway Functions, ETSI Standard ES 283 018 V1.1.4, October 2007*.

BGF Topology with Multiple Virtual BGFs and Gateway Controllers Overview

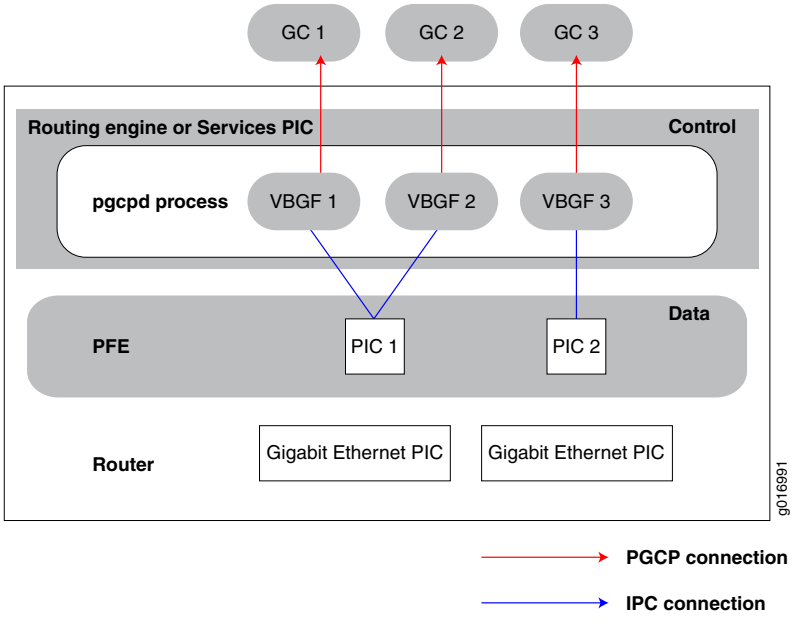
The BGF supports up to eight concurrent virtual BGFs in a router. Each virtual BGF is connected to a gateway controller over its own PGCP connection. One virtual BGF can connect to one gateway controller at the same time. Multiple virtual BGFs can share a single data service PIC and a single control service PIC. A single virtual BGF cannot span more than one data PIC or MS-DPC or more than one control PIC.

By creating multiple virtual BGFs, you can:

- Deploy different policy and quality of service (QoS) characteristics in your network.
- Scale your infrastructure by using multiple services PICs or MS-DPCs to control voice traffic.

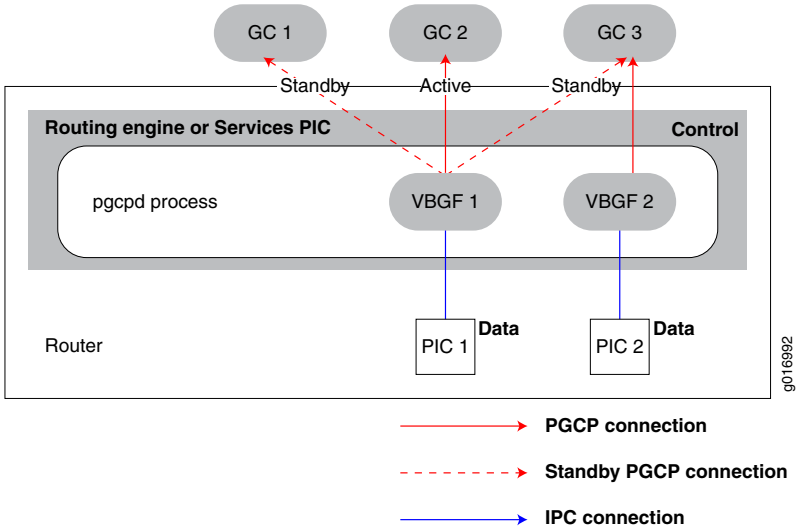
Figure 12 on page 43 shows a topology with multiple virtual BGFs and gateway controllers. This topology enables one virtual BGF and one MultiServices PIC to continue handling gate requests and forwarding packets on open gates even when the other PIC fails.

Figure 12: Topology with Multiple Virtual BGFs and Gateway Controllers



You can have multiple gateway controllers configured for one virtual BGF. When a virtual BGF begins running on the router, it attempts to set up a connection to the first configured gateway controller. Each virtual BGF can have one active gateway controller and one or more standby gateway controllers. In case of a gateway controller failure or in case of the gateway controller sending instructions to the virtual BGF, the virtual BGF can switch to another gateway controller. Figure 13 on page 44 shows an active and standby gateway controller connected to VBGF 2.

Figure 13: Active and Standby Gateway Controllers

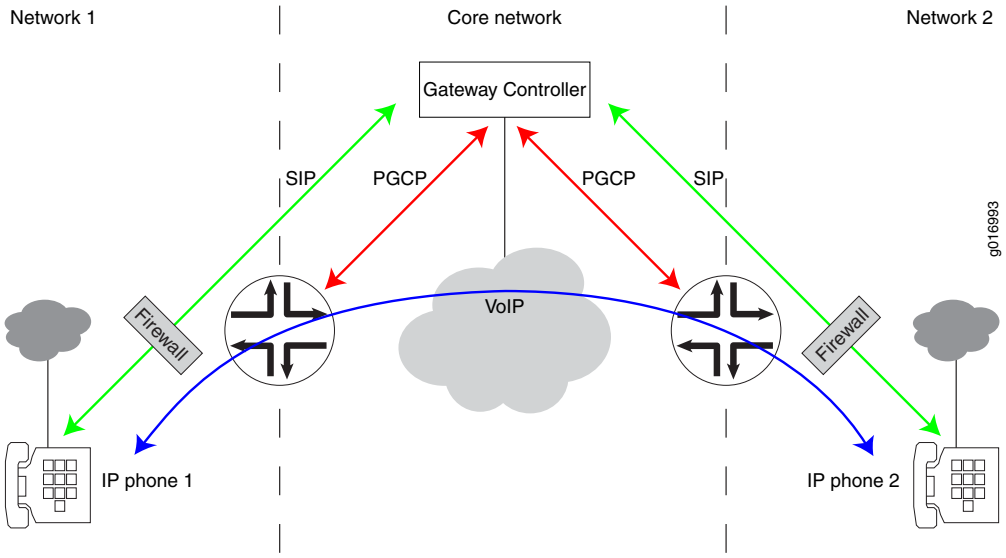


If the PGCP connection between the virtual BGF and the gateway controller is lost, the virtual BGF attempts to reconnect to the gateway controller. If the virtual BGF cannot reconnect to the gateway controller, it traverses its list of gateway controllers until it successfully connects to one of the gateway controllers.

Sample BGF Voice Network Topology

Figure 14 on page 45 shows a sample network that uses the BGF voice solution.

Figure 14: Sample BGF Voice Network

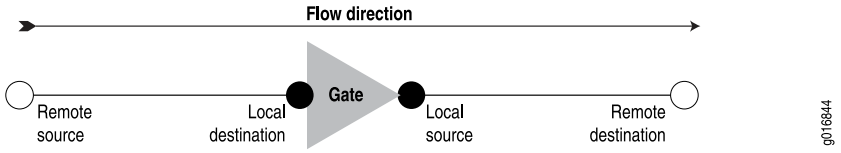


Control of Voice Flows with Gates Overview

The BGF uses gates to control voice flows in the transport plane. Gates are created through signaling instructions that the gateway controller provides to the BGF. Using the signaling instructions, the BGF 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 45 shows a unidirectional gate.

Figure 15: Unidirectional Gate

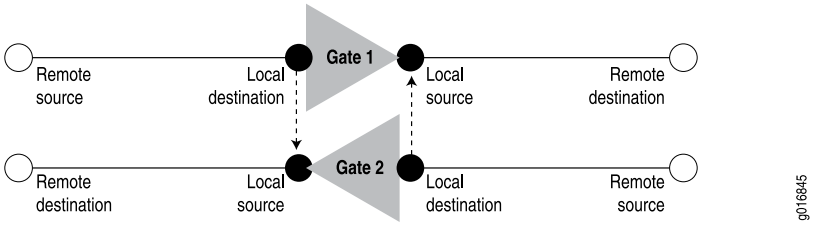


Gate Addressing

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

Figure 16 on page 46 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



Gate Opening, Closing, and Modification Overview

Based on information acquired through VoIP signaling, the gateway controller instructs the BGF through H.248 commands which gates to create and which actions to associate with them. Each gate can have many actions associated with it; for example, NAT, Differentiated Services (DiffServ) code point (DSCP) marking, and latching. The pgcpd process decodes H.248 commands that it receives from the gateway controller and uses IPC messages to instruct the PIC or DPC 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 or DPC:

- 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

Gate Identification

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

Forward and Drop Operations for RTP and RTCP Gates

You can use the StreamMode property in the LocalControl Descriptor of H.248 messages to change the mode of Realtime Transport Protocol (RTP) gates without affecting the mode of Real-Time Control Protocol (RTCP) gates. That is, you can put RTP gates in drop mode while leaving RTCP gates in forward mode.

To view whether RTP and RTCP gates are in drop mode or forward mode, use the show services pgcp flows command. The following example shows a gate in which the RTP stream is in drop mode, and the RTCP stream is in forward mode.

```
user@host>show services pgcp flows gateway bgf-1
Gate id: 4295033089
UDP      20.50.170.110:0     ->    20.50.170.2:1024 Drop I             0
    NAT source   20.50.170.110:0       ->     10.50.170.1:1024
    NAT dest       20.50.170.2:1024    ->   10.50.170.110:20000
Gate id: 4295033089
UDP      20.50.170.110:0     ->    20.50.170.2:1025 Forward I          0
    NAT source   20.50.170.110:0       ->     10.50.170.1:1025
    NAT dest       20.50.170.2:1025    ->   10.50.170.110:20001
```

Latch Deadlock and Media Inactivity Detection and Reporting

You can configure the parameters that a virtual BGF uses to detect and report latch deadlocks.

Detection

The virtual BGF uses an inactivity timer to detect a latch deadlock or other media inactivity on a gate. The timer tracks the receipt of media packets during a specified time interval.

When a latching signal exists for a termination, the BGF places the termination in a Drop state. All incoming traffic to the relevant gate egressing the termination is dropped until the first IP traffic datagram enters the termination (ingress). At this point the remote descriptor on the termination and egress gate is updated to forward traffic to the newly acquired source. The latch signal is removed from the gate when the gateway controller receives an H.248 Notify message containing the newly acquired IP address. Deadlock occurs when an error occurs regarding the source IP address and port that prevents the endpoint from returning data to the source address.

The detection process is activated in one of the following ways:

- The gateway controller requests quality (QUA) alerts.
- The gateway controller requests application data inactivity detection (ADID) alerts.
- The CLI is used to configure a forced service change when media inactivity occurs.

The inactivity timer tracks the receipt of media packets during a specified interval of time (inactivity duration). If no media packets are received during this time interval, the virtual BGF reports the inactivity to the gateway controller.

Reporting

Reporting of the media inactivity occurs in one of the following ways:

- If the virtual BGF detects a latch deadlock or media inactivity and you have configured the virtual BGF to force a service change, the virtual BGF stops service on the gate and sends the gateway controller a ServiceChange message using either error code 906 (Loss of Lower Layer Connectivity) or 910 (Media Capability Failure). The virtual BGF then takes the affected termination out of service, but does not subtract the termination.

- If you have not configured the virtual BGF to force a service change, the virtual BGF sends a QUA or ADID notification message, depending on which type of notification was requested by the gateway controller.

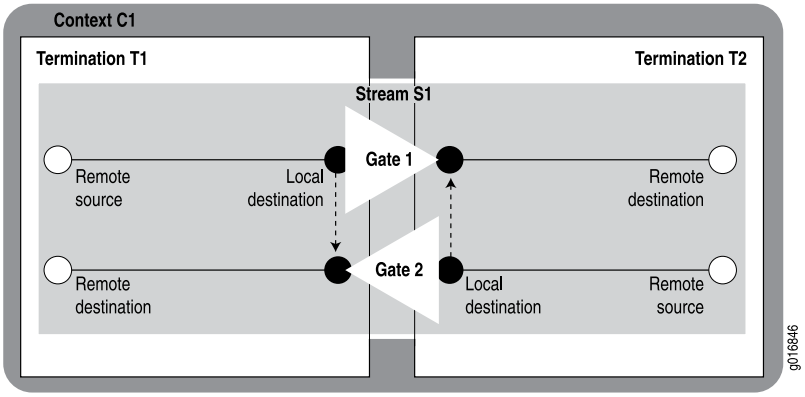
Related Topics

- Configuring Latch Deadlock and Media Inactivity Detection on page 79
- Monitoring Gates on page 97

H.248 Building Blocks Overview

The H.248 connection model uses contexts, terminations, and streams, which are logical entities that the gateway controller controls. In the router, the MultiServices PIC or MS-DPC creates a context. The software then adds terminations to the context and adds streams to the terminations. Figure 17 on page 48 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, subtract, modify, or audit commands. Terminations have unique identifiers (TerminationIDs) that the BGF 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 virtual BGF instructs a MultiServices PIC or MS-DPC to create a context for each voice session and each signaling session. Using instructions from the virtual BGF, the PIC or DPC then applies policies such as DSCP, NAT, rate limiting, and inactivity timers to the gates within a context. If the virtual BGF does not specify an existing context to which the termination is to be added, the PIC or DPC creates a new context.

Streams

A stream is one bidirectional flow within a context.

Virtual Interfaces with the BGF Overview

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

Included in the H.248 message exchange between the gateway controller and the virtual BGF is a virtual interface identifier. This identifier instructs the BGF which media resources to use.

Related Topics

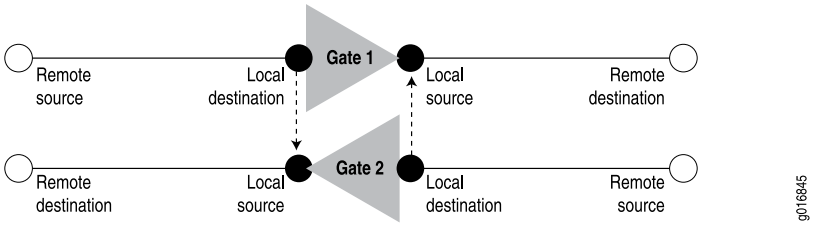
- Configuring Virtual Interfaces on page 70
- Example: Configuring the Virtual Interfaces on page 167

Twice NAT for VoIP Traffic Overview

The BGF 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 gates to achieve security between realms or service providers. To apply twice NAT, the pgcpd process instructs the PIC or DPC to allocate a specified number of NAT addresses and ports from a NAT pool on a per-gate basis. The pgcpd process specifies which NAT pool to use.

Figure 18 on page 49 shows two gates in a BGF.

Figure 18: Translation of Gate Addressing

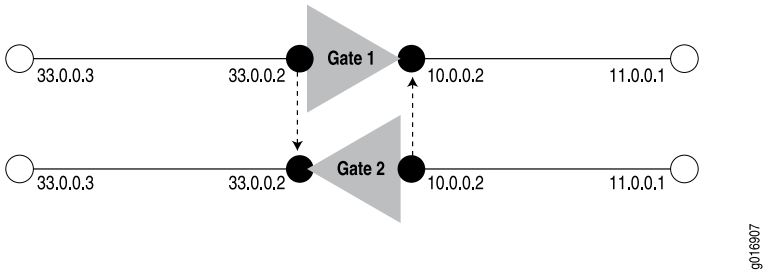


After flows are created for Gate 1, the gate connects the remote source to the local destination. The local source and local destination addresses reside on the router and must be uniquely specified. For Gate 1, twice NAT enables the router to translate the IP address of the remote source to the local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

Figure 19 on page 50 shows an example of how addresses are translated.

Figure 19: Example: Translation of Gate Addressing



NAT Pool Selection

You can configure separate NAT pools that can be controlled by either the BGF or the gateway controller. By default the BGF controls the addresses and ports in a pool. However, when you configure your NAT pool, you can specify that the gateway controller controls the addresses and ports in the NAT pool. The gateway controller reserves the addresses and ports when it requests specific local NAT bindings for remote addresses.

If the BGF selects the NAT pool, it can use one of the following methods to select the pool:

- (Default) Using the value of the media services assigned to virtual interfaces configured on the BGF.
- Matching the transport protocol type in H.248 messages received from the gateway controller.

NAT Pool Selection by Matching the Transport Protocol

The BGF can select the NAT pool by matching any combination of the following protocols:

- Real-Time Transport Protocol using Audio/Video profile (RTP/AVP)
- TCP
- UDP

Selecting a NAT pool based on transport protocol:

- Guarantees the prioritized distribution of network resources.
- Enables the use of multiple NAT pools for each virtual interface.

The gateway controller can set a transport protocol in the media description in the local descriptor command in Add and Modify commands that it sends to the BGF. The media description format is:

m=*media port transport format list*

where the *transport* field specifies the transport protocol. For example:

m=video 49170/2 RTP/AVP 31

When you set up your NAT pools, you specify a transport protocol or list of protocols. Do not configure the NAT pool to be remotely controlled by the gateway controller. Also, set the port in the NAT pool to automatic.

When the BGF receives an Add or Modify command with a media description, it searches the NAT pools associated with the virtual interface and attempts to match the transport protocols in the description with the transport protocols specified in the NAT pools. The BGF uses the first NAT pool that has a matching transport protocol. If it cannot find a match, it replies to the gateway controller with the following error:

ER=500 {"Application: Media handler not found"}

IPv4-to-IPv6 Address Translation

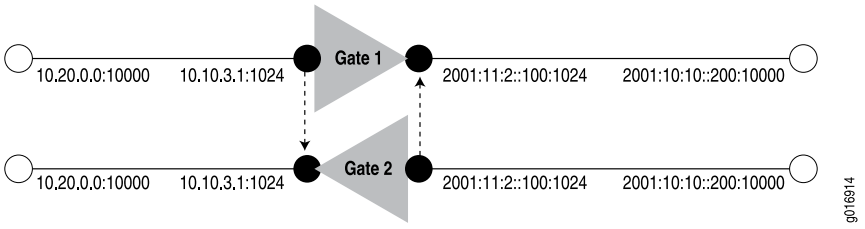
IPv4-to-IPv6 address translation enables callers in an IPv4 network to place calls to recipients in an IPv6 network. With this capability, the access side of the network can be an IPv4 network and the backbone side of the network can be an IPv6 network and vice versa. The gateway controller sets up gates so that one termination of the gate has IPv4 addresses and the other termination of the gate has IPv6 addresses. The BGF performs the appropriate IPv4-to-IPv6 and IPv6-to-IPv4 translations.

This implementation is not the tunnelling of IPv4 headers over IPv6 headers and vice versa. It is the translation of the IPv4 headers to IPv6 headers and vice versa.

You must configure both an IPv4 NAT pool and an IPv6 NAT pool on the BGF for IPv4-to-IPv6 translation to work.

Figure 20 on page 51 shows an example of a gate pair in a network where IPv4-to-IPv6 address translation is used.

Figure 20: IPv4-to-IPv6 Gates Using Twice NAT



Related Topics

- Configuring NAT Pools for the BGF on page 68
- Assigning a NAT Pool on page 70

- Example: Configuring NAT Pools on page 162
- Example: Assigning the NAT Pools to a Media Service on page 166

Quality of Service for VoIP Traffic Overview

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

You can configure a default DSCP value that the virtual BGF uses for outgoing traffic when the DSCP value is not defined by the gateway controller. If you do not configure a value, the default value is 0x00. All eight bits are exposed, but the packet uses only the six leading bits. You can embed other data in the other two bits.

The DiffServ package is defined in Annex A.2 of *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005*.

Related Topics

- Configuring QoS for the BGF on page 75
- Example: Configuring QoS for Voice Calls on page 172

Rate-Limiting for VoIP Traffic Overview

Because BGF 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.

The BGF provides a two-rate policer that you can apply to the ingress traffic of any gate.

This quality of service is provided through a two-rate three-color policing functionality on the MultiServices PIC or MS-DPC. This policer complies with *RFC 2698, A Two Rate Three Color Marker, September, 1999*. With the rate limiting capability, the MultiServices PIC or MS-DPC 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 gates. To enable rate limiting for a gate, you need to provide traffic management package (TMAN) parameters. You can configure these parameters in the JUNOS CLI (Table 5 on page 53) or they can come from the H.248 signaling commands received from the gateway controller. Traffic-management parameters that come from the gateway controller override parameters configured in the CLI.

Table 5: Traffic Parameters Configured in the CLI

Parameter	Description	Equivalent PGCP Signaling Command
Sustained data rate (SDR)	Provides the CIR	Tman/sdr
Peak data rate (PDR)	Provides the PIR	Tman/pdr
Maximum burst size (MBS)	Provides the burst size. Both the CBS and the PBS defined in RFC 2698 map to the maximum burst size.	Tman/mbs

For each of the traffic-management parameters, you can configure a value that applies to all gate streams and a value that applies only to RTCP gate streams. For RTCP streams, you can specify a fixed value for the parameters or you can specify the value as a percentage of the RTP rate. When RTP and RTCP are represented as a single stream, RTCP is policed whenever RTP is policed. You can also specify that RTCP bandwidth is be included in the SDR for streams other than RTCP.

The gateway controller can send traffic-management parameters to the BGF in gate open and gate modify signaling requests. When the PIC or DPC 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.
- Yellow if it exceeds the CIR.
- Green if it does not exceed the CIR.

Packets that are marked red are dropped by the PIC or DPC.

Default Values for Rate-Limiting Parameters

If the policy command H.248 message from the gateway controller is on (tman/pol = on), but the rate-limiting parameters are not specified in the message and the JUNOS rate-limiting parameters have not been configured, the BGF uses following default values:

- Peak data rate—10,000 bytes per second for all streams and 5 percent of the RTP gates' PDR for RTCP streams.
- Sustained data rate—10,000 bytes per second for all streams and 5 percent of the RTP gate's SDR for RTCP streams.

- Maximum burst size—1000 bytes for all streams and the MBS of the RTP gate for RTCP streams.

Rate Limiting and Fast Update Filters

When a VoIP flow configured through the BGF violates the SDR by three times the configured rate, fast update filters are installed on the gate to allow the rate-limiting drop action to occur on the PFE instead of the PIC or DPC.

A fast update filter is similar to a regular filter that is defined in the [edit firewall] hierarchy, except that the system can incrementally add or update terms.

For fast update filters, a term equals a gate definition. You can see gate definitions in the show services pgcp gates gateway command output.

The fast update filter match is performed based on the most specific defined term. For each filter, a default term is installed to allow traffic to pass through (otherwise, all traffic is dropped because it is the default firewall action). For example, two terms are listed when there are two filters.

Filters are in effect until the gate is destroyed. If the client loses its connection for over 30 seconds, the existing filters are deleted, and default fast update filters are installed.

Rate-Limiting Statistics Display

To display statistics for a gate including rate-limiting statistics and the number of packets dropped because of FUF filters, use the show services pgcp gate gateway *gateway-name* gate-id *gate-id* statistics command.

Related Topics

- Configuring Rate Limiting for the BGF on page 73
- Collecting Statistics on Gates with Rate-Limited Flows on page 100

Security for BGF Overview

The BGF feature provides the following security features:

- Interim AH scheme
- Symmetric control association

Interim AH Scheme

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 virtual BGF and the gateway controller. The interim AH scheme defines an authentication header with the H.248 protocol header.

To use the interim AH scheme, configure the security algorithm for the interim AH scheme for a gateway controller. If you configure an algorithm, the BGF accepts

H.248 messages from the gateway controller that include an AH from the defined algorithm. It discards received packets that do not include the expected AH. When the BGF replies to the gateway controller, it includes an AH from the defined algorithm.

Symmetric Control Association

For control association between the BGF and a gateway controller, you define the address and port of the BGF and the gateway controller. The BGF uses the address and port configured for the gateway controller when it sends registration messages to the gateway controller. If the registration reply contains a ServiceChangeAddress command, the BGF connects to the gateway controller using the new address or port or both instead of the address and port configured in the CLI. The BGF accepts only H.248 messages that arrive from the gateway controller address and port. All other messages are dropped.

In the following cases, the BGF attempts to connect to the address and port configured on the router:

- Loss of the BGF-to-gateway controller connection
- Restart of the pgcp-services
- Reboot of the router

If needed, the gateway controller can reply with a new ServiceChangeAddress command.

The BGF uses the new address in the ServiceAddressChange command only if the command is triggered by ServiceChangeReason 901 & 902. If the change is triggered by other ServiceChangeReasons such as 900, the BGF uses the configured address and port.

Related Topics

- Adding a Gateway Controller to the Virtual BGF Configuration on page 67

Priority and Emergency Call Handling

The gateway controller can set values for priority and emergency indicators for a context and include them in add or modify requests that it sends to the BGF. The BGF stores these priority and emergency values. The gateway controller can then query the BGF for context lists based on the priority and emergency settings. The BGF includes the priority and emergency properties in add or modify commands when the gateway controller requests a ContextAudit.

The BGF does not provide higher queuing and processing for emergency and priority calls.

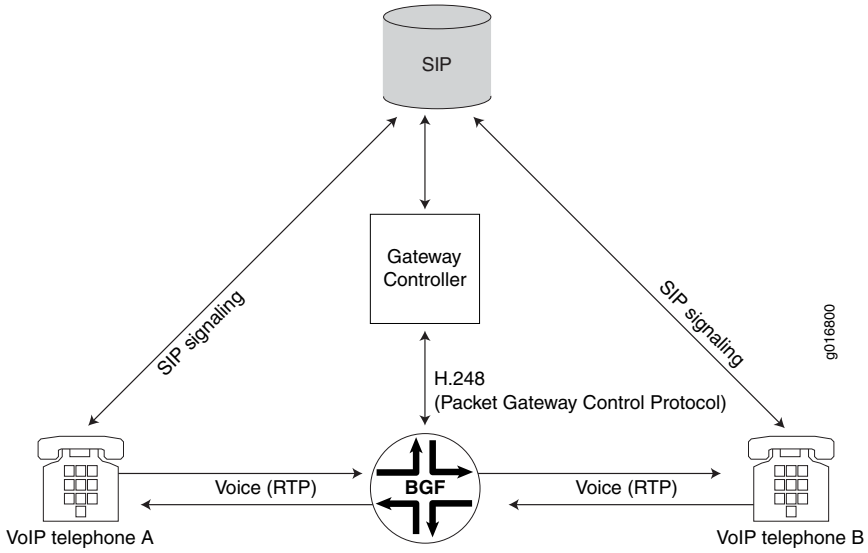
Related Topics
- Managing Overload Control with Priority Handling for Emergency Calls on page 121

BGF VoIP Call Setup Overview

As shown in Figure 21 on page 56, VoIP uses two streams:

- Signaling stream, which handles the agreement to set up calls. The signaling stream can use Session Initiation Protocol (SIP) or other signaling protocols.
- Media (RTP/RTCP) stream for each leg of the voice call.

Figure 21: Establishing a VoIP Call



The process of setting up a VoIP call in the network using SIP, as shown in Figure 21 on page 56, is as follows:

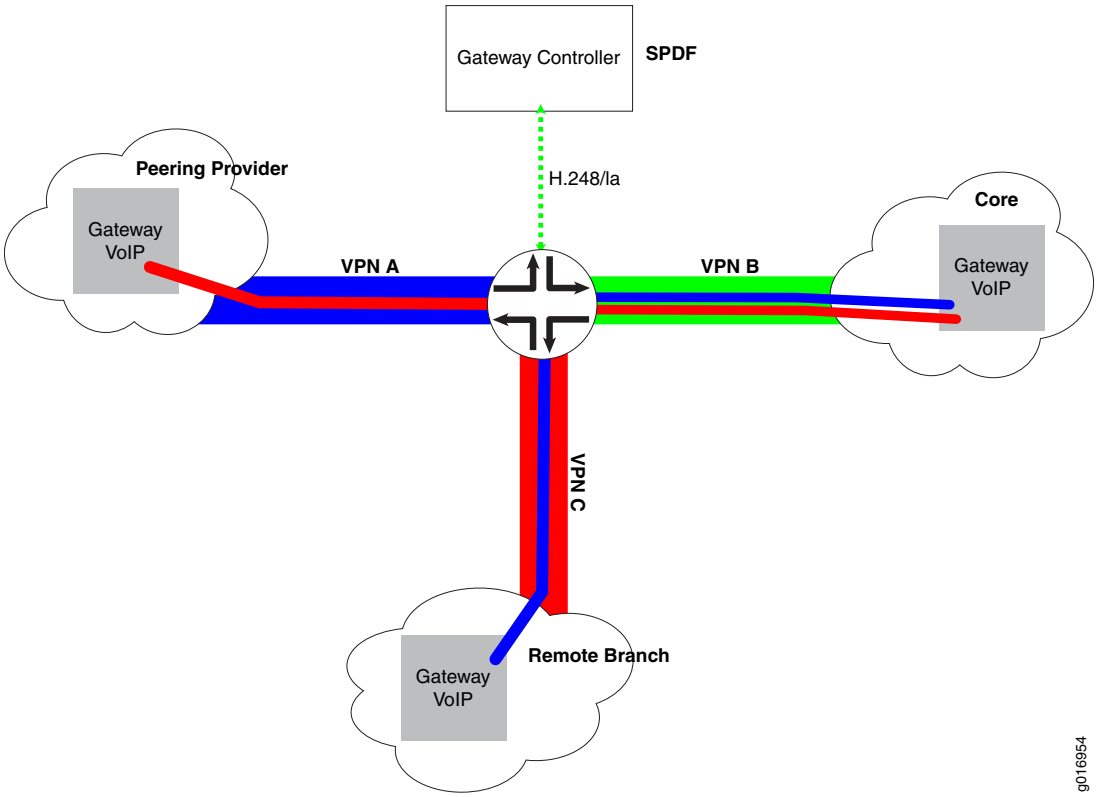
1. VoIP telephone A initiates a VoIP call to VoIP telephone B.
2. VoIP telephone A sends a SIP message to the SIP server.
3. The gateway controller (SIP server) sends an H.248 request for gate allocation from the virtual BGF.
4. The pgcpd process running on the Routing Engine sends IPC messages to the MultiServices PIC or MS-DPC requesting that the PIC or DPC open gates for each call leg.
5. The PIC or DPC creates the gates with the behaviors specified in the IPC messages, and it sends a reply to the pgcpd process. Gates are allocated in a Drop state.
6. The virtual BGF sends an H.248 response providing allocated gate information to the gateway controller.
7. The SIP server sends the modified SIP signaling (based on the gate information sent by the virtual BGF) to the destination VoIP telephone B.

8. VoIP telephone B replies to the SIP request to the SIP server.
9. The gateway controller updates the virtual BGF with the new information sent by VoIP telephone B.
10. Steps 4-6 are repeated, where the PIC or DPC is updated with the new information provided by the gateway controller. Gates are transitioned into a Forward state.
11. The SIP server sends the modified reply to VoIP telephone A.
12. The call is established. Media streams can now flow through the routers' open gates.

VPN Aggregation for VoIP Calls Overview

The VPN aggregation feature uses VPN routing and forwarding (VRF) so users on one VPN can call users on another VPN. For example, in Figure 22 on page 57, users in VPN B can call users in VPN A and VPN C.

Figure 22: VPN Aggregation in a VoIP Network



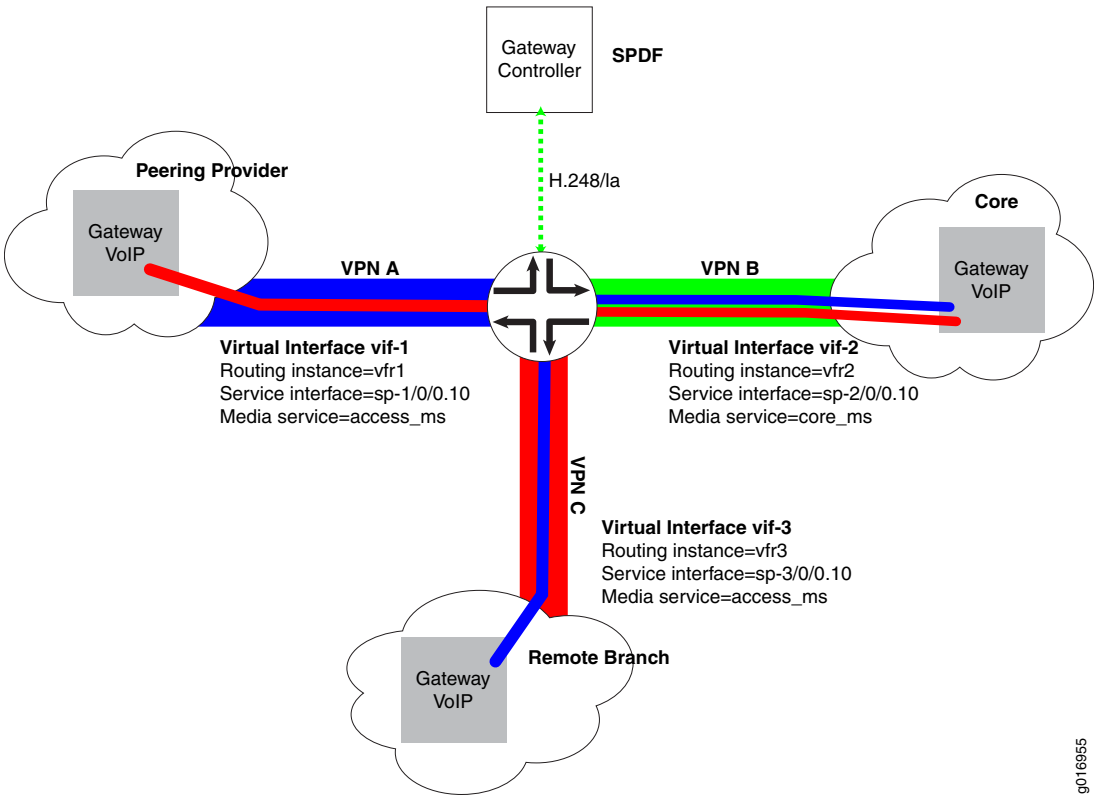
VPN aggregation provides the following benefits:

- Provides a scalable way to configure VRFs in a mesh-like configuration that uses only one logical service interface for each VRF.
- Reduces the number of service sets that you need because you can add all of your logical service interfaces to a pool of interfaces, and then assign the entire pool of interfaces to a service set.
- Configurations are inline so, when you provision the service set for VRFs, you can seamlessly tie the service into the BGF service without the need for additional configuration states.
- Uses the router's native support for VRFs and VPNs, which omits the need for an external element that terminates the VRFs and replaces them with the VLAN tags required to support VoIP media handling.

How VPN Aggregation Works

VPN aggregation uses the virtual interface configurations as shown in Figure 23 on page 58 to route traffic from users in one VPN to users in another VPN.

Figure 23: Overview of VPN Aggregation Configuration



The VPN aggregation configuration consists of:

- VRFs—One for each VPN. The VRF is required to create a layer 3 VPN. The VRF must have the instance type of VRF, a logical service interface, a route distinguisher, and VRF import and export policies.
- Pool of logical service interfaces—One pool that contains all service interfaces that are configured in your VRF routing instances. Instead of explicit inside and outside service interfaces, all of the interfaces in the pool can be both inside and outside service interfaces.
- Service Set—One service set that has a next-hop service set to the pool of logical service interfaces and that contains a PGCP rule. The service set links the VRFs to the PGCP service.
- Virtual interface—One for each VRF routing instance. The virtual interface configuration establishes the relationship between the following parts of the configuration:
  - NAT pool (the media service contains the NAT pool)
  - VRF routing instance to which the NAT routes are added
  - The service interface

When a gate is established, the pgcpd process uses the virtual interface information in the termination ID to determine the ingress and egress virtual interfaces for the gate. In turn, the virtual interface configuration maps to the VRF, NAT pool, and service interface.

The termination IDs of the caller and the call recipient contain the virtual interface ID. For example, in Figure 23 on page 58 termination ID ip/4/vif-1/1 matches virtual interface vif-1, which is mapped through the configuration to routing instance vrf1.

Related Topics

- Configuring VPN Aggregation on page 76

Session Mirroring Overview

Session mirroring allows you to send a copy of a context to an external device called a delivery function for analysis. With session mirroring, the original session is sent to its intended destination and the mirrored session is sent to the delivery function. The mirroring operations are transparent to the user whose session is being mirrored.

Session mirroring is supported for IPv4 and IPv6 traffic. IPv6 packets that are mirrored are encapsulated in IPv4 headers.

The BGF can mirror up to 1 percent of gates at a time.

Activation of Session Mirroring for a Gate

When session mirroring is enabled, the BGF uses information in H.248 requests received from the gateway controller to identify sessions to be mirrored and to trigger the mirroring session. The following sample H.248 request includes session-mirroring information:

```
MEGACO/2 [123.123.123.3]:2944
Transaction = 10003 {
    Context = $ {
        Add = $ {
            Media {
                LocalControl {
                    Mode = SendReceive,
                    li/LICn=ff00ff00ff00ff00},
                    li/LITID = [ffffff00, ffffff01],
                Remote {
                        v=0
                        c=IN IP4 124.124.124.222
                        m=audio 2222 RTP/AVP 0
                        a=ptime:20
                    }
                }
        }
    }
}
```

- The LICn command provides an encrypted correlation number. The pgcpd process decrypts the correlation number to determine whether session mirroring is performed on the gate. If the number is valid, interception is performed on the gate. If the number is invalid, no interception is performed on the gate.
- The LITID command contains one or more target IDs that identify the recipients of mirrored packets. If the request contains multiple LITIDs, a copy of mirrored packets is created for each target ID. All copies are sent to the same delivery function. A maximum number of seven copies is supported for each packet.

How Session Mirroring Works

If session mirroring is required on a gate, the pgcpd process embeds appropriate data in the gate open/modify request that it sends to the PIC or DPC. This data includes direction information to indicate whether the packet is mirrored before applying NAT actions or after. It also includes the decrypted correlation number and Target IDs that need to be embedded in the packet sent to the delivery function.

The PIC or DPC then:

1. Marks the gate that needs to be mirrored and obtains the destination for the mirrored packets from the CLI configuration.
2. Processes the packets as it normally does. It applies DSCP, latching, and rate limiting as appropriate.
    - Additional mirrored packets that are sent as a result of session mirroring do not impact rate limiting. The replicated packets do not count against policer counters that are used to compute the rate for the gate.
    - Mirrored packets are sent with DSCP marks that are applied to the gate as they are for a normal flow.
    - If the original packet is dropped because of rate limiting; no mirroring occurs.
    - Latch or relatch actions on the gate do not impact mirroring.

3. Generates one copy of the packets received on mirrored gates for each target ID specified in the H.248 request, encapsulates the mirrored packets, and sends them to the configured delivery function.

Session mirroring can be enabled or disabled any time during a gate's life by employing H.248 commands. If mirroring is enabled in one stream of a termination, all streams in the context are mirrored. Both RTP and RTCP packets are mirrored for a gate marked for mirroring.

Security for Packets Sent to the Delivery Function

To protect mirrored traffic that is sent from the BGF to the delivery function, you can use IPsec.

Related Topics

- Configuring Session Mirroring on page 85
- Displaying Gates That Are Being Mirrored on page 101

Chapter 4

Configuring the BGF

This chapter explains how to configure the voice solution. Topics include:

Configuring Virtual BGFs to Run on Services PICs

By default virtual BGFs run on the Routing Engine. If you plan to run virtual BGFs on a MultiServices PIC or MultiServices Dense Port Concentrator (MS-DPC) instead of on the Routing Engine, you need to enable the BGF service package on the PIC or DPC and then configure the service interface that you want to run the pgcpd process.

Enabling the BGF Service Package on the PIC or DPC

Step-by-Step Procedure To enable the BGF service package on a PIC or DPC:

1. Determine the FPC slot number and the PIC number of the services PIC or DPC on which you want to enable the BGF service package.

   In the following example, the FPC slot number is 0 and the PIC number is 3.

   ```
   user@host>show chassis hardware
   Hardware inventory:
   Item          Version  Part number  Serial number     Description
   .
   .
   .
   FPC 0                                E-FPC
     PIC 0       REV 11   750-002971   RH1375           4x OC-3 SONET, MM
     PIC 1       REV 12   750-012838   DN0449           4x 1GE(LAN), IQ2
       Xcvr 0    REV 01   740-013111   8142659           SFP-T
       Xcvr 1    REV 01   740-013111   8142630           SFP-T
       Xcvr 2    REV 01   740-013111   8155199           SFP-T
       Xcvr 3    REV 01   740-013111   8154799           SFP-T
     PIC 2       REV 11   750-005724   RH2051           2x OC-3 ATM-II IQ, MM
     PIC 3       REV 15   750-014895   DN3277           MultiServices 100
   .
   .
   .
   ```

2. Enable the jservices-bgf package on the PIC or DPC.

   ```
   [edit chassis]
   user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
     package jservices-bgf
   ```

3. Set the number of megabytes that can be used for the wired process memory, which is virtual memory used to reduce Translation Look-aside Buffer (TLB) misses.

   ```
   [edit chassis]
   user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
     wired-process-mem-size 512
   ```

4. Set the number of processing cores dedicated to the control functionality of the jservices-bgf application.

   ```
   [edit chassis]
   user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
     control-cores 7
   ```

5. Specify that the PIC or DPC not restart if the routing engine is swapped.

   ```
   [edit chassis]
   user@host#set no-service-pic-restart-on-failover
   ```

6. Commit your configuration changes. You must perform the commit before you can proceed to configure the BGF.

```
[edit]
user@host#commit
commit complete
```

Configuring the Control Services PIC or DPC for the Virtual BGF

To run the virtual BGF on a MultiServices PIC or MS-DPC, you need to configure the service interface that you want to run the pgcpd process.

Step-by-Step Procedure To configure the PIC or MS-DPC:

1. Enter edit mode for the interface.

```
[edit]
user@host#edit interfaces ms-0/3/0
```

2. Configure a description for the interface.

```
[edit interfaces ms-0/3/0]
user@host#set description BGF-Service-PIC
```

3. Configure logical unit 0, and specify the protocol family and the address of a virtual BGF.

```
[edit interfaces ms-0/3/0]
user@host#set unit 0 family inet address 10.10.200.21/32
```

4. Configure a logical unit and specify the protocol family.

```
[edit interfaces ms-0/3/0]
user@host#set unit 10 family inet
```

5. Configure a logical unit and specify the protocol family.

```
[edit interfaces ms-0/3/0]
user@host#set unit 20 family inet
```

Related Topics

- *Chapter 24, Interface Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 25, Summary of Interface Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Virtual BGF

You can configure eight virtual BGFs on a router.

Step-by-Step Procedure To configure a virtual BGF:

1. Create a virtual BGF, and assign a name to the virtual BGF. You can configure an IP address as the virtual BGF name. However, the IP address is not used in the operation of the virtual BGF.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1
   ```

2. Specify whether the virtual BGF runs on the Routing Engine or on a service device, either a MutliServices PIC or an MS-DPC. By default, the virtual BGF runs on the Routing Engine.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set platform device ms-0/3/0
   ```

3. Specify the IP address of the virtual BGF. This address is the local IP address on which the virtual BGF receives H.248 messages from the gateway controller.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set gateway-address 10.10.30.1
   ```

4. Specify the port number of the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set gateway-port 2944
   ```

5. Configure the number of seconds before the virtual BGF removes gates following a disconnection from the gateway controller.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set cleanup-timeout 3600
   ```

6. Configure the maximum number of concurrent calls allowed on the virtual BGF. If you configure multiple virtual BGFs for one PIC or DPC, you can use this statement to achieve intentional oversubscription of resources or a fair distribution of resources between the virtual BGFs.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set max-concurrent-calls 3000
   ```

NOTE:

To change the max-concurrent-calls for a virtual BGF that is in service, you must:

1. Take the virtual BGF out of service by initiating a graceful or forced shutdown. For more information, see “Shutting Down a Virtual BGF” on page 116.
2. Configure the new value for max-concurrent-calls.
3. Put the virtual BGF in service. See “Making the Virtual BGF Operational Again” on page 116.
4. Restart the pgcpd process. See “Restarting the pgcpd Process Running on the Routing Engine” on page 113.

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- Example: Configuring the Virtual BGFs on page 160

Adding a Gateway Controller to the Virtual BGF Configuration

To configure a gateway controller for a virtual BGF, specify the IP address and port number of the gateway controller. You can also secure the connection by specifying an algorithm for the interim AH scheme.

Step-by-Step Procedure

To configure a gateway controller for a virtual BGF:

1. Access the configuration of the virtual BGF for which you want to add a gateway controller.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1
   ```

2. Create a gateway controller configuration, and assign a name to the gateway controller. You can configure an IP address as the gateway controller name. However, the IP address is not used for the connection to the gateway controller.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#edit gateway-controller gc-1
   ```

3. Specify that the gateway controller is a remote gateway controller.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set remote-controller
   ```

4. Specify the IP address of the gateway controller.

   ```
   [edit services pgcp gateway bgf-1 gateway-controller gc-1]
   user@host#set controller-address 10.10.2.3
   ```

5. Configure the number of the gateway controller listening port. The virtual BGF sends H.248 messages to this port.

   ```
   [edit services pgcp gateway bgf-1 gateway-controller gc-1]
   user@host#set controller-port 2944
   ```

6. To use the interim authentication header (AH) scheme to provide security on the PGCP connection, configure the security algorithm that the interim AH scheme uses. Currently, HMAC null is the only algorithm supported.

   ```
   [edit services pgcp gateway bgf-1 gateway-controller gc-1]
   user@host#set interim-ah-scheme algorithm hmac-null
   ```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring NAT Pools for the BGF

You can configure a network address translation (NAT) pool that is exclusive to the BGF. This topic shows how to create the following types of NAT pools:

- Configuring a Remotely Controlled NAT Pool on page 68
- Configuring a NAT Pool Selected Based on Transport Protocol on page 69

Configuring a Remotely Controlled NAT Pool

Step-by-Step Procedure To configure a remotely controlled NAT pool:

1. Create a NAT pool, and specify a name for the pool.

   ```
   [edit services]
   user@host#edit nat pool bgf-pool
   ```

2. Configure an address range for the pool.

   ```
   [edit services nat pool bgf-pool]
   user@host#set address-range low 10.10.20.100 high 10.10.30.100
   ```

3. Configure a range of ports. If you configure the NAT pool as remotely controlled, you must set a specific port range rather than using an automatic assignment of ports.

   ```
   [edit services nat pool bgf-pool]
   user@host#set port range low 10000 high 50000
   ```

4. Specify that the NAT pool is used exclusively by the BGF.

   ```
   [edit services nat pool bgf-pool]
   user@host#set pgcp
   ```

5. Specify that the gateway controller controls the addresses and ports in a NAT pool. The gateway controller reserves the addresses and ports when it requests specific local NAT bindings for remote addresses. (By default, the BGF controls the addresses and ports in a pool.)

   ```
   [edit services nat pool bgf-pool]
   user@host#set pgcp remotely-controlled
   ```

6. Configure the number of ports allocated to voice and video flows on the MultiServices PIC or MS-DPC. This value is useful when one port is allocated for Real-Time Transport Protocol (RTP), and the accompanying Real-Time Control Protocol (RTCP) flow uses the other port. By default, 2 ports are available. To support the extra ports required for combined voice and video flows, you can specify 4 ports.

   ```
   [edit services nat pool bgf-pool]
   ```

```
user@host#set pgcp ports-per-session 4
```

Configuring a NAT Pool Selected Based on Transport Protocol

Step-by-Step Procedure To configure a NAT pool that can be selected based on its transport protocol:

1. Create a NAT pool, and specify a name for the pool.

   ```
   [edit services]
   user@host#edit nat pool bgf-pool
   ```

2. Configure an address range for the pool.

   ```
   [edit services nat pool bgf-pool]
   user@host#set address-range low 10.10.20.100 high 10.10.30.100
   ```

3. Configure a range of ports. If you configure the NAT pool as remotely controlled, you must set a specific port range rather than using an automatic assignment of ports.

   ```
   [edit services nat pool bgf-pool]
   user@host#set port range low 10000 high 50000
   ```

4. Specify that the NAT pool is used exclusively by the BGF.

   ```
   [edit services nat pool bgf-pool]
   user@host#set pgcp
   ```

5. Specify one or more transport protocols that must match the transport protocol in the media descriptor of Add or Modify requests from the gateway controller.

   ```
   [edit services nat pool bgf-pool]
   user@host#set pgcp transport [rtp-avp udp]
   ```

6. Specify that the port is automatically assigned.

   ```
   [edit services nat pool bgf-pool]
   user@host#set port automatic
   ```

7. Configure the number of ports allocated to voice and video flows on the MultiServices PIC or MS-DPC. This value is useful when one port is allocated for Real-Time Transport Protocol (RTP), and the accompanying Real-Time Control Protocol (RTCP) flow uses the other port. By default, 2 ports are available. To support the extra ports required for combined voice and video flows, you can specify 4 ports.

   ```
   [edit services nat pool bgf-pool]
   user@host#set pgcp ports-per-session 4
   ```

Related Topics

- *Chapter 9, Summary of Network Address Translation Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- Twice NAT for VoIP Traffic Overview on page 49

Assigning a NAT Pool

To assign a NAT pool, you create a media service configuration that contains the name of the NAT pool. You then specify the media service in a virtual interface configuration and in a BGF rule. The BGF rule assigns the media service for a specific virtual BGF.

Step-by-Step Procedure To configure a media service:

1. Create a media service, and specify a name for the service.

   ```
   [edit services pgcp]
   user@host#edit media-service media-service-one
   ```

2. Assign the NAT pool to the media service.

   ```
   [edit services pgcp media-service media-service-one]
   user@host#set nat-pool bgf-pool
   ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Virtual Interfaces

A virtual interface provides the mapping between interface names that appear in the H.248 termination ID in H.248 messages and the media service to be used for a gate.

Step-by-Step Procedure To configure a virtual interface:

1. Create a virtual interface, and specify a name for the interface.

   ```
   [edit services pgcp]
   user@host#edit virtual-interface 1
   ```

2. Specify the name of the media service that contains the NAT pool to be used for gates on the virtual interface that you are configuring.

   ```
   [edit services pgcp virtual-interface 1]
   user@host#set media-service media-service-one
   ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Creating a Rule That Specifies the NAT Pool to Use on a Virtual BGF

Rules for the BGF are applied on the MultiServices PIC or MS-DPC. The rules combined with firewall rules specify how to deal with VoIP media traffic. The BGF rules specify the NAT pool (media service) used on a specific virtual BGF.

Step-by-Step Procedure To configure a rule:

1. Create a rule and specify a name for the rule.

   ```
   [edit services pgcp]
   user@host#edit rule bgf-rule-1
   ```

2. Specify the virtual BGF on which this rule is applied.

   ```
   [edit services pgcp rule bgf-rule-1]
   user@host#set gateway bgf-1
   ```

3. Specify the media service that contains the NAT pool to be used for this virtual BGF.

   ```
   [edit services pgcp rule bgf-rule-1]
   user@host#set media-service media-service-one
   ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Specifying the Order in Which the BGF Processes Rules

If you have defined multiple rules, you can specify the order in which the BGF processes the rules by creating a rule set. The BGF processes the rules in the order in which you specify them in the rule set. It processes rules as follows:

- If a rule matches the packet, the BGF performs the corresponding action and the rule processing stops.
- If no rule matches the packet, processing continues to the next rule in the set. If none of the rules match the packet, the packet is dropped by default.

Step-by-Step Procedure

To configure a rule set.

1. Create a rule set and specify a name for the rule set.

   ```
   [edit services pgcp]
   user@host#edit rule-set bgf-rule-set-1
   ```

2. Add a rule to the rule set.

   ```
   [edit services pgcp rule-set bgf-rule-set-1]
   user@host#set rule bgf-rule-1
   ```

3. Add additional rules to the rule set.

   ```
   [edit services pgcp rule-set bgf-rule-set-1]
   user@host#set rule bgf-rule-2
   ```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Stateful Firewall for the BGF

Step-by-Step Procedure To create a stateful firewall:

1. Create a stateful firewall rule.

   ```
   [edit services stateful-firewall]
   user@host#edit rule r1
   ```

2. Set the match direction for the rule.

   ```
   [edit services stateful-firewall rule r1]
   user@host#set match-direction input-output
   ```

3. Add a term to the rule.

   ```
   [edit services stateful-firewall rule r1]
   user@host#set term t1 then reject
   ```

Related Topics
- *Chapter 7, Summary of Stateful Firewall Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Service Set

A service set allows you to combine directional rules, stateful firewall rules, CoS rules, and other rules that control the behavior of each service in the service set. Unless you are configuring the service set to be used with VPN aggregation, we recommend you configure the service set for the BGF as a next-hop service set that specifies the inside and outside logical service interfaces on the MultiServices PIC or MS-DPC. You need to configure a service set for each PIC or DPC.

Step-by-Step Procedure To configure a service set:

1. Create a service set configuration.

   ```
   [edit services]
   user@host#edit service-set bgf-svc-set
   ```

2. Configure service set as a next-hop service set.

   ```
   [edit services service-set bgf-svc-set]
   user@host#edit next-hop-service
   ```

3. Specify the service interface to the inside network. The interface must be a logical interface on the same MultiServices PIC or MS-DPC and must not be used by another service set. This unit number must match the unit number of the inside service domain configured in the service interface.

   ```
   [edit services service-set bgf-svc-set next-hop-service]
   ```

```
user@host#set inside-service-interface sp-1/2/0.10
```

4. Specify the service interface to the outside network. The interface must be a logical interface on the same PIC or DPC and must not be used by another service set. This unit number must match the unit number of the outside service domain configured in the service interface.

```
[edit services service-set bgf-svc-set next-hop-service]
user@host#set outside-service-interface sp-1/2/0.20
```

5. Specify the name of the BGF rule or rule set that applies to this service set.

```
[edit services service-set bgf-svc-set]
user@host#set pgcp-rules bgf-rule-1
```

6. Specify the name of the stateful firewall rule that applies to this service set.

```
[edit services service-set bgf-svc-set]
user@host#set stateful-firewall-rules r1
```

7. Specify the name of the CoS rule that applies to this service set.

```
[edit services service-set bgf-svc-set]
user@host#set cos-rules cos-rule
```

8. Configure logging for the service set.

```
[edit services service-set bgf-svc-set]
user@host#edit syslog host local-1
[edit services service-set bgf-svc-set syslog host local-1]
user@host#set services any
```

Related Topics

- *Chapter 22, Service Set Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 23, Summary of Service Set Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Rate Limiting for the BGF

You can configure rate limiting for voice calls on the virtual BGF by setting default, minimum, and maximum values for properties defined in the H.248 traffic management package. The virtual BGF uses the default values unless the gateway controller overrides them with an H.248 command. You can configure maximum and minimum values if you want to limit the range of values accepted from the gateway controller. Parameters for the RTCP stream take effect only when the gate is an RTP/RTCP gate. You can configure peak and sustained data rates for the RTCP stream as a set rate or as a percentage of the corresponding RTP data rate.

The traffic management package is defined in Annex C of *Gateway control protocol v3, ITU-T Recommendation H.248.53, — June 2008.*

Step-by-Step Procedure To configure rate limiting for the gate stream and the RTCP stream:

1. Access the configuration of the H.248 traffic-management properties.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#edit h248-properties traffic-management
   ```

2. Configure a peak data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set peak-data-rate default 3000000
   ```

3. Configure the maximum acceptable peak data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set peak-data-rate maximum 3500000
   ```

4. Configure the minimum acceptable peak data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set peak-data-rate minimum 2500000
   ```

5. Configure a separate peak data rate for RTCP gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set peak-data-rate rtcp fixed-value 100000
   ```

6. Configure a sustained data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set sustained-data-rate default 2000000
   ```

7. Configure the maximum acceptable sustained data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set sustained-data-rate maximum 2500000
   ```

8. Configure the minimum acceptable sustained data rate for all gate streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set sustained-data-rate minimum 1500000
   ```

9. Optionally specify that rtcp bandwidth be included in the sustained data rate for all streams.

   ```
   [edit services pgcp gateway bgf-1 h248-properties traffic-management]
   user@host#set sustained-data-rate rtcp-include
   ```

10. Configure a sustained data rate for RTCP gate streams.

    ```
    [edit services pgcp gateway bgf-1 h248-properties traffic-management]
    user@host#set sustained-data-rate rtcp fixed-value 200000
    ```

11. Configure a maximum burst size for all gate streams.

    ```
    [edit services pgcp gateway bgf-1 h248-properties traffic-management]
    user@host#set max-burst-size default 3000000
    ```

12. Configure the maximum acceptable maximum burst size for all gate streams.

```
[edit services pgcp gateway bgf-1 h248-properties traffic-management]
user@host#set max-burst-size maximum 3500000
```

13. Configure the minimum acceptable maximum burst size for all gate streams.

```
[edit services pgcp gateway bgf-1 h248-properties traffic-management]
user@host#set max-burst-size minimum 2500000
```

14. Configure a maximum burst size for RTCP gate streams.

```
[edit services pgcp gateway bgf-1 h248-properties traffic-management]
user@host#set max-burst-size rtcp percentage 1000
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring QoS for the BGF

Step-by-Step Procedure To configure a default DSCP value:

1. Access the configuration of the H.248 DiffServ properties.

```
[edit services pgcp gateway bgf-1]
user@host#edit h248-properties diffserv
```

2. Configure a value for the DSCP.

```
[edit services pgcp gateway bgf-1 h248-properties diffserv]
user@host#set dscp default ef
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring the Data Services PIC or MS-DPC

You need to configure a service interface that is a logical interface on an Adaptive Services (AS) PIC, a MultiServices PIC, or an MS-DPC.

Step-by-Step Procedure To configure the service interface:

1. Configure the interface, and enter edit mode for the interface.

```
[edit interfaces]
user@host#edit sp-1/2/0
```

2. Configure a description for the interface.

```
[edit interfaces sp-1/2/0]
user@host#set description bgf_service
```

3. Configure logical unit 0.

```
[edit interfaces sp-1/2/0]
user@host#set unit 0 family inet
```

4. Configure a logical unit and specify the protocol family.

```
[edit interfaces sp-1/2/0]
user@host#set unit 10 family inet
```

5. Set the service domain of the logical unit to inside. This unit number must match the unit number of the inside service interface configured in the service set.

```
[edit interfaces sp-1/2/0]
user@host#set unit 10 service-domain inside
```

6. Configure a logical unit and specify the protocol family.

```
[edit interfaces sp-1/2/0]
user@host#set unit 20 family inet
```

7. Set the service domain of the logical unit to outside. This unit number must match the unit number of the outside service interface configured in the service set.

```
[edit interfaces sp-1/2/0]
user@host#set unit 20 service-domain outside
```

8. Configure system logging on the service interface.

```
[edit interfaces sp-1/2/0]
user@host#set services-options syslog host local services any
```

9. Configure an inactivity timeout for sessions on the service interface.

```
[edit interfaces sp-1/2/0 services-options syslog]
user@host#set services-options inactivity-timeout 720
```

Related Topics

- *Chapter 24, Interface Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 25, Summary of Interface Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring VPN Aggregation

VPN aggregation configurations have the following requirements.

- All interfaces in a pool must belong to the same service PIC.
- Logical interfaces cannot be in more than one pool.
- All interfaces must have either family inet or family inet6 configured.
- Logical unit 0 cannot be configured in a service interface pool.
- The maximum number of service interfaces in a pool is 1000.

- The service set must have a next-hop service that is set to the service interface pool; it cannot have inside and outside services.
- The service set must have a BGF rule.
- In the virtual interface configuration, the service interface must match the interface configured in the VRF routing instance.
- The virtual interface configuration must include all media services in the BGF rule that is configured in the service set.

Step-by-Step Procedure

See Figure 23 on page 58 for an illustration of this configuration.

To configure VPN Aggregation:

1. Configure a policy statement to be used for the vrf-import and vrf-export policies that you plan to configure in the routing instances.

```
[edit]
user@host#edit policy-options policy-statement policy-1

[edit policy-options policy-statement policy-1]
user@host#set term t1 then reject
```

2. Configure a VRF routing instance for each VPN.

```
[edit]
user@host#edit routing-instances vrf1

[edit routing-instances vrf1]
user@host#set instance-type vrf
user@host#set interface sp-1/0/0.10
user@host#set route-distinguisher 10.10.10.11:0
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1

[edit]
user@host#edit routing-instances vrf2

[edit routing-instances vrf2]
user@host#set instance-type vrf
user@host#set interface sp-2/0/0.10
user@host#set route-distinguisher 10.10.10.22:0
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1

[edit]
user@host#edit routing-instances vrf3

[edit routing-instances vrf3]
user@host#set instance-type vrf
user@host#set interface sp-3/0/0.10
user@host#set route-distinguisher 10.10.10.33:0
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1
```

3. Configure a pool of logical service interfaces that are configured in the VRF routing instances.

```
[edit]
user@host#edit services service-interface-pools pool bgf-pool

[edit services service-interface-pools pool bgf-pool
user@host#set interface sp-1/0/0.10
user@host#set interface sp-2/0/0.10
user@host#set interface sp-3/0/0.10
```

4. Create a service set that links the VRF and the BGF services. Specify the service interface pool as the next-hop service. The service set must contain a BGF rule. It cannot contain any other type of rule.

```
[edit]
user@host#edit services service-set bgf

[edit services service-set bgf]
user@host#set next-hop-service service-interface-pool bgf-pool
user@host#set pgcp-rules bgf-rule
```

5. Configure a virtual interface for each VRF routing instance.

```
[edit]
user@host#edit services pgcp virtual-interface 1

[edit services pgcp virtual-interface 1]
user@host#set routing-instance vrf1 service-interface sp-1/0/0.10
user@host#set media-service access_ms

[edit]
user@host#edit services pgcp virtual-interface 2

[edit services pgcp virtual-interface 2]
user@host#set routing-instance vrf2service-interface sp-2/0/0.10
user@host#set media-service core_ms

[edit]
user@host#edit services pgcp virtual-interface 3

[edit services pgcp virtual-interface 3]
user@host#set routing-instance vrf3 service-interface sp-3/0/0.10
user@host#set media-service access_ms
```

Related Topics

- VPN Aggregation for VoIP Calls Overview on page 57
- *JUNOS VPNs Configuration Guide*
- *Chapter 23, Summary of Service Set Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 29, Summary of Service Interface Pools Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Latch Deadlock and Media Inactivity Detection

The gateway can request to be notified by the virtual BGF when a latching deadlock or media inactivity exists on a gate. You can configure latching deadlock and media inactivity detection parameters for use by the virtual BGF when it monitors media traffic that is flowing through the gate.

Latch deadlock detection is defined in *Gateway Control Protocol: Application Data Inactivity Package, ITU-T Recommendation H.248.40, January, 2007.*

Step-by-Step Procedure To configure parameters for latching deadlock and media inactivity detection:

1. Access the configuration of your virtual BGF and specify data-inactivity-detection.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1 data-inactivity-detection
   ```

2. Configure the number of seconds before the virtual BGF begins checking for media inactivity on new gates for which there is a latching signal.

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#set latch-deadlock-delay 10
   ```

3. Configure the number of seconds before the virtual BGF begins checking for media inactivity on new gates that do not have a latching signal.

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#set inactivity-delay 10
   ```

4. Configure the duration of inactivity detection checks that the virtual BGF performs on a gate. If no media packets are received during a check, the virtual BGF sends the gateway controller a quality (QUA) alert, ADID alert, or service change notification. If media packets are received, the timer is reset and checking continues. This parameter applies to all gates, regardless of whether there is a latching signal for the gate.

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#set inactivity-duration 60
   ```

5. Configure the virtual BGF to stop inactivity detection when a gate action is set to drop. Use this option to handle calls that are placed on hold. When calls are resumed, the BGF starts the delay timer and resumes data inactivity detection. By default, inactivity detection continues when a gate is ready to drop

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#set stop-detection-on-drop
   ```

6. Specify that a notification (or service change) occur immediately when no media packets are detected during the initial checking delay period (latch-deadlock-delay or inactivity-delay). By default, inactivity is not reported until the delay period and an inactivity duration period have elapsed.

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#set send-notification-on-delay
   ```

7. Request a service change to take gates with latch deadlocks or media inactivity out of service, dropping all packets for the gates. Specify whether to notify the gateway controller with error code 906 (loss of lower layer connectivity) or 910 (media capability failure).

   ```
   [edit services pgcp gateway bgf-1 data-inactivity-detection]
   user@host#edit report-service-change

   [edit services pgcp gateway bgf-1 data-inactivity-detection report-service-change]
   user@host#set service-change-type forced-910
   ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring H.248 Timers

You can configure H.248 timers for the PGCP connection between the virtual BGF and the gateway controller. See clause 9.2 and annex D of the *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005*, for details about these timers.

Step-by-Step Procedure

To configure H.248 timers for the PGCP connection between the virtual BGF and the gateway controller:

1. Access the configuration of the H.248 timers.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1 h248-timers
   ```

2. Configure the value of the average acknowledgment delay (AAD) that the virtual BGF uses before the first AAD is measured.

   ```
   [edit services pgcp gateway bgf-1 h248-timers]
   user@host#set initial-average-ack-delay 1000
   ```

3. Configure the assumed maximum network propagation delay time.

   ```
   [edit services pgcp gateway bgf-1 h248-timers]
   user@host#set maximum-net-propagation-delay 5000
   ```

4. Configure a maximum waiting delay (MWD) that is used when the virtual BGF attempts to reconnect to the gateway controller. If the virtual BGF finishes traversing its list of gateway controllers, and has not connected to a controller, the virtual BGF waits for a random value between 0 and MWD milliseconds before it attempts to reconnect to a gateway controller.

   ```
   [edit services pgcp gateway bgf-1 h248-timers]
   user@host#set maximum-waiting-delay 10000
   ```

5. Configure the maximum time that a transaction can be kept alive. When this time expires, the BGF considers the gateway controller to be down.

   ```
   [edit services pgcp gateway bgf-1 h248-timers]
   user@host#set tmax-retransmission-delay 25000
   ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring H.248 Base Root Properties

You can configure default, minimum, and maximum values for properties defined in the H.248 base root package. The virtual BGF uses the default values unless the gateway controller overrides them with an H.248 command. You can configure maximum and minimum values to limit the range of values accepted from the gateway controller. In general, we recommend you use the values that are configured on the router by default.

The base root package is defined in annex E.2 of the *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005*. The properties in this package mostly affect the timers used when the virtual BGF and gateway controller send and receive provisional responses to H.248 commands.

Step-by-Step Procedure

To configure H.248 timers for the PGCP connection between the virtual BGF and the gateway controller:

1. Access the configuration of the H.248 base root properties.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1 h248-properties base-root
   ```

2. Set the default value for the number of milliseconds for the gateway controller to wait for a response to transactions from the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1 h248-properties base-root]
   user@host#set normal-mg-execution-time default 600
   ```

3. Set the minimum value for the number of milliseconds for the gateway controller to wait for a response to transactions from the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1 h248-properties base-root]
   user@host#set normal-mg-execution-time minimum 500
   ```

4. Set the maximum value for the number of milliseconds for the gateway controller to wait for a response to transactions from the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1 h248-properties base-root]
   user@host#set normal-mg-execution-time maximum 1000
   ```

5. Set the default value for the number of milliseconds for the gateway controller to wait for a pending response from the virtual BGF if a transaction cannot be completed.

   ```
   [edit services pgcp gateway bgf-1 h248-properties base-root]
   user@host#set mg-provisional-response-timer-value default 1000
   ```

6. Set the minimum value for the number of milliseconds for the gateway controller to wait for a pending response from the virtual BGF if a transaction cannot be completed.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mg-provisional-response-timer-value minimum 500
```

7. Set the maximum value for the number of milliseconds for the gateway controller to wait for a pending response from the virtual BGF if a transaction cannot be completed.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mg-provisional-response-timer-value maximum 2000
```

8. Set the default value for the number of transaction pending messages that the gateway controller can receive from the virtual BGF.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mg-originated-pending-limit default 10
```

9. Set the minimum value for the number of transaction pending messages that the gateway controller can receive from the virtual BGF.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mg-originated-pending-limit minimum 4
```

10. Set the maximum value for the number of transaction pending messages that the gateway controller can receive from the virtual BGF.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mg-originated-pending-limit maximum 20
```

11. Set the default value for the number of milliseconds for the virtual BGF to wait for a response to transactions from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set normal-mgc-execution-time default 1000
```

12. Set the minimum value for the number of milliseconds for the virtual BGF to wait for a response to transactions from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set normal-mgc-execution-time minimum 500
```

13. Set the maximum value for the number of milliseconds for the virtual BGF to wait for a response to transactions from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set normal-mgc-execution-time maximum 2000
```

14. Set the default value for the number of milliseconds for the virtual BGF to wait for a pending response from the gateway controller if a transaction cannot be completed.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-provisional-response-timer-value default 4000
```

15. Set the minimum value for the number of milliseconds for the virtual BGF to wait for a pending response from the gateway controller if a transaction cannot be completed.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-provisional-response-timer-value minimum 1000
```

16. Set the maximum value for the number of milliseconds for the virtual BGF to wait for a pending response from the gateway controller if a transaction cannot be completed.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-provisional-response-timer-value maximum 8000
```

17. Set the default value for the number of transaction pending messages that the virtual BGF can receive from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-originated-pending-limit default 10
```

18. Set the minimum value for the number of transaction pending messages that the virtual BGF can receive from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-originated-pending-limit minimum 4
```

19. Set the maximum value for the number of transaction pending messages that the virtual BGF can receive from the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-properties base-root]
user@host#set mgc-originated-pending-limit maximum 100
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring H.248 Segmentation Properties

You can configure default, minimum, and maximum values for properties defined in the H.248 segmentation package. The virtual BGF uses the default values unless the gateway controller overrides them with an H.248 command. You can configure maximum and minimum values to limit the range of values accepted from the gateway controller. In general, we recommend you use the values that are configured on the router by default.

The segmentation package is defined in annex E.14 of the *Gateway control protocol v3, ITU T Recommendation H.248.1, September 2005*. The properties in this package affect the limits used when long H.248 replies are segmented into several H.248 messages.

Step-by-Step Procedure

To configure default values for H.248 segmentation properties:

1. Access the configuration of the H.248 segmentation properties.

```
[edit services pgcp ]
user@host#edit gateway bgf-1 h248-properties segmentation
```

2. Set a default value for the number of milliseconds for the gateway controller to wait for outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken message.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-segmentation-timer default 4000**

3. Set a minimum value for the number of milliseconds for the gateway controller to wait for outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken message.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-segmentation-timer minimum 2000**

4. Set a maximum value for the number of milliseconds for the gateway controller to wait for outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken message.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-segmentation-timer maximum 8000**

5. Set a default value, in bytes, for the MG maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the gateway controller sends to the BGF.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-maximum-pdu-size default 1472**

6. Set a minimum value, in bytes, for the MG maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the gateway controller sends to the BGF.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-maximum-pdu-size minimum 736**

7. Set a maximum value, in bytes, for the MG maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the gateway controller sends to the BGF.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mg-maximum-pdu-size maxmum 7360**

8. Set a default value for the number of milliseconds for the virtual BGF to wait for outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mgc-segmentation-timer default 4000**

9. Set a minimum value for the number of milliseconds for the virtual BGF to wait for outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken.

   [edit services pgcp gateway bgf-1 h248-properties segmentation]
   user@host#**set mgc-segmentation-timer minimum 2000**

10. Set a maximum value for the number of milliseconds for the virtual BGF to wait for outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken.

    ```
    [edit services pgcp gateway bgf-1 h248-properties segmentation]
    user@host#set mgc-segmentation-timer maximum 8000
    ```

11. Set a default value, in bytes, for the MGC maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the virtual BGF sends to the gateway controller.

    ```
    [edit services pgcp gateway bgf-1 h248-properties segmentation]
    user@host#set mgc-maximum-pdu-size default 1472
    ```

12. Set a minimum value, in bytes, for the MGC maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the virtual BGF sends to the gateway controller.

    ```
    [edit services pgcp gateway bgf-1 h248-properties segmentation]
    user@host#set mgc-maximum-pdu-size minimum 736
    ```

13. Set a maximum value, in bytes, for the MGC maximum PDU size property of the segmentation package. This value determines the maximum size of messages that the virtual BGF sends to the gateway controller.

    ```
    [edit services pgcp gateway bgf-1 h248-properties segmentation]
    user@host#set mgc-maximum-pdu-size maximum 7360
    ```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Session Mirroring

Session mirroring commands are hidden by default. You must have a login with sufficient permission to configure session mirroring. The set system login class *class-name* permissions pgcp-session-mirroring-control command grants this permission.

Step-by-Step Procedure

To configure session mirroring:

1. Access the configuration of the delivery function properties under session-mirroring.

    ```
    [edit services pgcp ]
    user@host#edit session-mirroring delivery-function df-1
    ```

2. Configure the network operator ID. The BGF includes the network operator ID in the header of intercepted packets that it sends to the delivery function. It is used to identify the operator.

    ```
    [edit services pgcp session-mirroring delivery-function df-1]
    user@host#set network-operator-id ABCDE
    ```

3. Configure the address of the delivery function to which the BGF sends session-mirroring information.

```
[edit services pgcp session-mirroring delivery-function df-1]
user@host#set destination-address 10.1.1.63
```

4. Configure the port on the delivery function that receives session-mirroring information.

```
[edit services pgcp session-mirroring delivery-function df-1]
user@host#set destination-port 15000
```

5. Configure the address of the interface on which the BGF sends session-mirroring data to the deliver function.

```
[edit services pgcp session-mirroring delivery-function df-1]
user@host#set source-address 10.1.1.43
```

6. Configure the port on which the BGF sends session-mirroring data to the delivery function.

```
[edit services pgcp session-mirroring delivery-function df-1]
user@host#set source-port 10000
```

Disabling Session Mirroring

To disable session mirroring:

```
[edit services pgcp session-mirroring]
user@host#set disable-session-mirroring
```

Re-Enabling Session Mirroring

To re-enable session mirroring:

```
[edit services pgcp session-mirroring]
user@host#delete disable-session-mirroring
```

Configuring IPsec for Mirrored Sessions

To protect mirrored traffic that is sent from the BGF to the delivery function, you can use IPsec. To have IPsec and the BGF on the same PIC, you create BGF and IPsec service sets and chain these service-sets using routing-options.

To create the service sets and routing options:

1. Configure a service set for the BGF. The NAT routes installed as part of BGF service direct PGCP traffic to sp-1/0/0.10 and sp-1/0/0.20.

```
[edit services service-set bgf-svc-set]
user@host#set pgcp-rules bgf-rule
user@host#set next-hop-service inside-service-interface sp-1/0/0.10
user@host#set next-hop-service outside-service-interface sp-1/0/0.20
```

2. Configure an IPsec service set on the same PIC.

```
[edit services service-set ipsec-svc-set]
```

```
user@host#set next-hop-service inside-service-interface sp-1/0/0.30
user@host#set next-hop-service outside-service-interface sp-1/0/0.40
user@host#set ipsec-vpn-options local-gateway 1.0.0.1
user@host#set ipsec-vpn-rules ipsec1
```

3. Install a static route to the delivery function (1.0.0.3) with the next-hop address of the PIC. This route redirects mirrored packets to a unit of the same service PIC that is hosting the IPsec service.

```
[edit]
user@host#set routing-options static route 1.0.0.3/32 next-hop sp-1/0/0.30
```

The mirrored packets that are generated on sp-1/0/0 have the destination address of the delivery function, which in this case is 1.0.0.3.

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Verifying Your Configuration

You can use show commands to verify your configuration.

Verifying the BGF Configuration

Purpose Display the current configuration of the BGF.

Action

```
[edit services pgcp]
user@host# show
media-service media-service-one {
    nat-pool bgf-pool;
}
virtual-interface 1 {
    media-service media-service-one;
}
gateway bgf-1 {
    gateway-address 10.10.30.1;
    gateway-port 2944;
    cleanup-timeout 3600;
    h248-timers {
        maximum-waiting-delay 10000;
        tmax-retransmission-delay 25000;
```

```
    initial-average-ack-delay 1000;
    maximum-net-propagation-delay 5000;
}
h248-properties {
    base-root {
        normal-mg-execution-time {
            default 600;
            minimum 500;
            maximum 1000;
        }
        mg-provisional-response-timer-value {
            default 1000;
            minimum 500;
            maximum 2000;
        }
        mg-originated-pending-limit {
             default 10;
            minimum 4;
            maximum 20;
        }
        normal-mgc-execution-time {
            default 1000;
            minimum 500;
            maximum 2000;
        }
        mgc-provisional-response-timer-value {
            default 4000;
            minimum 1000;
             maximum 8000;
        }
        mgc-originated-pending-limit {
             default 10;
             minimum 4;
             maximum 100;
        }
    }
    segmentation {
        mgc-segmentation-timer {
             default 4000;
             minimum 2000;
             maximum 8000;
        }
        mgc-maximum-pdu-size {
             default 1472;
             minimum 736;
             maximum 7360;
        }
             default 4000;
             minimum 2000;
             maximum 8000;
        }
        mg-maximum-pdu-size {
             default 1472;
             minimum 736;
             maximum 7360;
        }
    }
    diffserv {
        dscp {
            default ef;
        }
```

```
        }
        traffic-management {
            sustained-data-rate {
                 default 2000000;
                 minimum 1500000;
                 maximum 2500000;
                 rtcp {
                    fixed-value 200000;
                 }
            }
            peak-data-rate {
                  default 3000000;
                  minimum 2500000;
                  maximum 3500000;
                 rtcp {
                    fixed-value 100000;
                  }
            }
            max-burst-size {
                 default 3000000;
                 minimum 2500000;
                 maximum 3500000;
                 rtcp {
                     percentage 1000;
                 }
            }
        }
    }
    max-concurrent-calls 6000;
    gateway-controller gc-1 {
        controller-address 10.10.2.3;
        controller-port 2944;
        interim-ah-scheme {
            algorithm hmac-null;
        }
        remote-controller;
    }
    data-inactivity-detection {
        inactivity-delay 10;
        latch-deadlock-delay 10;
        send-notification-on-delay;
        inactivity-duration 60;
        stop-detection-on-drop;
        report-service-change {
            service-change-type forced-910;
        }
    }
}
rule bgf-rule-1 {
    gateway bgf-1;
    media-service media-service-one;
}
rule bgf-rule-2 {
    gateway bgf-1;
    media-service media-service-one;
}
rule-set bgf-rule-set-1 {
    rule bgf-rule-1;
    rule bgf-rule-2;
}
session-mirroring {
```

```
    delivery-function df-1 {
        destination-address 10.1.1.63;
        destination-port 15000;
        network-operator-id ABCDE;
        source-address 10.1.1.43;
        source-port 10000;
    }
}
```

Verifying the BGF Service Package Configuration

If you configured your virtual BGFs to run on a services PIC, verify that the BGF services package is installed on the services interface.

Purpose Display the chassis configuration.

Action

```
[edit chassis]
user@host# show
chassis {
    no-service-pic-restart-on-failover;
    fpc 0 {
        pic 3 {
            adaptive-services {
                service-package {
                    extension-provider {
                        control-cores 7;
                        wired-process-mem-size 512;
                        package jservices-bgf;
                    }
                }
            }
        }
    }
}
```

Verifying the Control Service PIC Configuration

If you configured your virtual BGFs to run on a services PIC, verify that the Control Service PIC is configured.

Purpose Display the control service PIC configuration.

Action

```
[edit interfaces]
user@host# show
ms-0/3/0 {
    description BGF-Service-PIC;
    unit 10 {
        family inet;
        service-domain inside;
    }
    unit 20 {
        family inet;
        service-domain outside;
    }
}
```

Verifying the Service Interface Configuration

Purpose Display the service interface configuration.

Action
```
[edit interface sp-1/0/0]
user@host# show
description bgf_service;
traceoptions {
    flag all;
}
services-options {
    syslog {
        host local {
            services any;
        }
    }
    inactivity-timeout 720;
}
unit 0 {
    family inet;
}
unit 10 {
    family inet;
    service-domain inside;
}
unit 20 {
    family inet;
    service-domain outside;
}
```

Verifying the Service Set Configuration

Purpose Display the service set configuration.

Action
```
[edit services service-set bgf-svc-set]
user@host# show
syslog {
    host local-1 {
        services any;
    }
}
stateful-firewall-rules r1;
cos-rules cos-rule;
pgcp-rules bgf-rule-1;
next-hop-service {
    inside-service-interface sp-1/2/0.10;
    outside-service-interface sp-1/2/0.20;
}
```

Verifying the NAT Pool Configuration

Purpose Display the NAT pool configuration for a remotely controlled NAT pool.

Action
```
[edit services nat]
user@host# show
```

```
pool bgf-pool {
    pgcp {
        remotely-controlled;
        ports-per-session 4;
    }
    address-range low 10.10.20.100 high 10.10.30.100;
    port range low 10000 high 50000;
}
```

Purpose Display the NAT pool selected based on transport protocol.

Action
```
[edit services nat]
user@host# show
pool bgf-pool {
    pgcp {
        ports-per-session 4;
        transport [ rtp-avp udp ];
    }
    address-range low 10.10.20.100 high 10.10.30.100;
    port automatic;
}
```

Verifying the Stateful Firewall Configuration

Purpose Display the stateful firewall configuration.

Action
```
[edit services stateful-firewall]
user@host# show
rule r1 {
    match-direction input-output;
    term t1 {
        then {
            reject;
        }
    }
}
```

Verifying the VPN Aggregation Configuration

Purpose Display the policy options configuration.

Action
```
[edit policy-options]
user@host# show
policy-statement policy-1 {
    term t1 {
        then reject;
    }
}
```

Purpose Display the routing instance configuration

Action
```
[edit routing-instances]
user@host# show
vrf1 {
    instance-type vrf;
    interface sp-1/0/0.10;
```

```
    route-distinguisher 10.10.10.11:0;
    vrf-import policy-1;
    vrf-export policy-1;
}
vrf2 {
    instance-type vrf;
    interface sp-2/0/0.10;
    route-distinguisher 10.10.10.22:0;
    vrf-import policy-1;
    vrf-export policy-1;
}
vrf3 {
    instance-type vrf;
    interface sp-3/0/0.10;
    route-distinguisher 10.10.10.33:0;
    vrf-import policy-1;
    vrf-export policy-1;
}
```

Purpose Display the service interface pool configuration.

Action

```
[edit services service-interface-pools]
user@host# show
pool vrf-pool {
    interface sp-1/0/0.10;
    interface sp-2/0/0.10;
    interface sp-3/0/0.10;
}
```

Purpose Display the service set configuration.

Action

```
[edit services service-set bgf]
user@host# show
pgcp-rules bgf-rule;
next-hop-service {
    service-interface-pool vrf-pool;
}
```

Purpose Display the virtual interface.

Action

```
[edit services pgcp]
user@host# show
virtual-interface 1 {
    routing-instance vrf1 service-interface sp-1/0/0.10;
    media-service access_ms;
}
virtual-interface 2 {
    routing-instance vrf1 service-interface sp-2/0/0.10;
    media-service core_ms;
}
virtual-interface 3 {
    routing-instance vrf3 service-interface sp-3/0/0.10;
    media-service access_ms;
}
```

Chapter 5

Monitoring the BGF

This chapter explains how to monitor the BGF components. Topics include:

Monitoring RTP and RTCP Traffic

To monitor Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) packets on media gates, the virtual BGF uses RTP and RTCP application layer gateway (ALGs) that are attached to flows when the gateway controller installs media gates on the virtual BGF.

The RTP ALG uses the sequence number of each RTP packet on that flow to record the number of lost packets. Each RTP packet contains a 16-bit sequence number field that is incremented for every packet sent. The starting sequence number is randomly selected.

The RTCP ALG monitors the Sender Report and Receiver Report packet types. For the sender, the ALG records the Synchronization Source (SSRC) value and the number of invalid packets, sender packets, and sender octets.

For the receiver, the RTCP ALG records monitors lost packets, the fraction of lost packets, and jitter. When the ALG tracks multiple receiver reports (that is, when a sender is listening to media from multiple sources), it tracks the statistics for up to four sources. When more than four sources are available, the ALG overwrites the statistics for the source with the oldest record.

Enabling Monitoring of RTP and RTCP Traffic

You can enable RTP and RTCP ALGs for twice NAT flows created when the gateway controller installs media gates on the virtual BGF. The ALGs monitor packets on the gate and provide statistics.

You can enable these ALGs only for flows created by the virtual BGF. You cannot enable them within standalone NAT rules.

Step-by-Step Procedure

You can choose to monitor either RTP or RTCP, or both. To enable monitoring of RTP and RTCP media flows:

1. Access the configuration of your virtual BGF.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1
   ```

2. Enable monitoring of both RTP and RTCP for media flows.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set monitor media
   ```

3. Enable monitoring of only RTP media flows.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set monitor media rtp
   ```

4. Enable monitoring of only RTCP media flows.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set monitor media rtcp
   ```

5. In operational mode, view statistics gathered for RTP and RTCP.

```
user@host> show services pgcp gate gateway bgf-1 gate-id 352187384065
statistics

Gate Statistics:
================
Output packets: 582
Input packets: 582
Dropped packets: 0
Lost RTP packets: 0

RTCP statistics:

SSRC           : 32270
Sender octets  : 7500
Sender packets : 375
Invalid packets: 9

RTCP Receiver statistics:

SSRC        Lost packets   Lost fraction         Jitter
13043                  0           0.000              0
16487                  0           0.000              0
5655                   0           0.000              0

. . .
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Monitoring Gates

Use the following topics to learn about monitoring gates:

Displaying Information About All Gates on a Virtual BGF

Purpose Display information about all gates on a virtual BGF using the show services pgcp gates gateway *gateway-name* command.

Action

```
user@host> show services pgcp gates gateway bgf-1
Virtual BGF configuration:
  Name                                    :  bgf-1
  IP address                              :  3.0.0.2
  Port                                    :  2944
  Status                                  :  Connected

Gate information:
Gate id: 4295033088
Gate state: Active
Service set id: 1
Media card: sp-0/3/0
Media handler: bgf-svc-set-1
Termination-id-string: ip/0/rlmvi2/1

Gate id: 4295033089
Gate state: Active
Service set id: 1
Media card: sp-0/3/0
Media handler: bgf-svc-set-1
Termination-id-string: ip/0/rlmvi0/2

Gate id: 8590000384
Gate state: Active
Service set id: 1
Media card: sp-0/3/0
Media handler: bgf-svc-set-1
Termination-id-string: ip/0/rlmvi2/3

Gate id: 8590000385
```

```
Gate state: Active
Service set id: 1
Media card: sp-0/3/0
Media handler: bgf-svc-set-1
Termination-id-string: ip/0/rlmvi0/4
```

Displaying Extensive Information About All Gates on a Virtual BGF

Purpose Display information about all gates on a virtual BGF including statistics for the gates, RTCP sender and RTCP receiver statistics, and rate-limiting statistics for the gates, using the show services pgcp gates gateway *gateway-name* extensive command.

Action

```
user@host> show services pgcp gates gateway bgf-1 extensive
Virtual BGF configuration:
  Name                                    :  bgf-1
  IP address                              :  2.0.0.2
  Port                                    :  2944
  Status                                  :  In-Service (Registered)

Gate information:
================
Gate id: 4295033088
Gate state: active
Direction: A->B
Action: forward
Remote source address: *
Remote source port: *
Remote destination address: 4.0.0.1
Remote destination port: 5060
Local source address: [4.99.99.20]
Local source port: [5060]
Local destination address: 2.99.99.20
Local destination port: 5060
Transport: udp
RTCP: Off
Latch: none
DSCP: 0x00 (Effective 0)
Policing: On
Gate SDR : 10000 bytes per second
Gate PDR : 10000 bytes per second
Gate MBS : 1000 bytes
RTCP SDR : 500 bytes per second
RTCP PDR : 500 bytes per second
RTCP MBS : 1000 bytes
Fast update filter: Off

Gate information:
================
Gate id: 4295033089
Gate state: active
Direction: B->A
Action: forward
Remote source address: *
Remote source port: *
Remote destination address: 2.0.0.1
Remote destination port: 5060
Local source address: [2.99.99.20]
Local source port: [5060]
Local destination address: 4.99.99.20
```

```
Local destination port: 5060
Transport: udp
RTCP: Off
Latch: none
DSCP: 0x00 (Effective 0)
Policing: On
Gate SDR : 10000 bytes per second
Gate PDR : 10000 bytes per second
Gate MBS : 1000 bytes
RTCP SDR : 500 bytes per second
RTCP PDR : 500 bytes per second
RTCP MBS : 1000 bytes
Fast update filter: Off
```

Displaying the Number of Gates Installed on a Virtual BGF

Purpose Display the number of gates installed on a virtual BGF using the show services pgcp gates gateway *gateway-name* count command.

Action

```
user@host> show services pgcp gates gateway bgf-1 count
Gateway Name                                        Gate count
bgf-1                                                    4
```

Displaying Information About a Specific Gate

Purpose Display information about a specific gate using the show services pgcp gate gateway *gateway-name* gate-id *gate-id* command.

Action

```
user@host> show services pgcp gate gateway bgf-1 gate-id 4295033089

Gate information:
Gate id: 4295033089
Gate state:  active
Action: forward
Service set id: 1
Media card: sp-0/2/0
Media handler: bgf-svc-set
Termination-id-string: ip/0/rlmvi2/1
```

Displaying Extensive Information About a Specific Gate

Purpose Display extensive information about a specific gate including statistics for the gate using the show services pgcp gate gateway *bgf-1* gate-id *gate-id* extensive command.

Action

```
user@host> show services pgcp gate gateway bgf-1 gate-id 4295033089 extensive
Gate information:
================
Gate id: 4295033089
Gate state: active
Direction: B->A
Action: forward
Remote source address: *
Remote source port: *
Remote destination address: 2.0.0.1
Remote destination port: 5060
```

```
Local source address: [2.99.99.20]
Local source port: [5060]
Local destination address: 4.99.99.20
Local destination port: 5060
Transport: udp
RTCP: Off
Latch: none
DSCP: 0x00 (Effective 0)
Policing: On
Gate SDR : 10000 bytes per second
Gate PDR : 10000 bytes per second
Gate MBS : 1000 bytes
RTCP SDR : 500 bytes per second
RTCP PDR : 500 bytes per second
RTCP MBS : 1000 bytes
Fast update filter: Off
```

Displaying Statistics for Gates

Purpose Display statistics for a gate, including packet statistics, RTCP sender and RTCP receiver statistics, rate-limiting statistics, and the number of packets dropped because of fast update filters (FUF), using the show services pgcp gate gateway *gateway-name* gate-id *gate-id* statistics command.

Action

```
user@host> show services pgcp gate gateway bgf-1 gate-id 98784313601 statistics
Gate Statistics:
================
Output packets: 0
Input packets: 0
Dropped packets: 0
Lost RTP packets: 0

Rate limiting statistics:

Mark Color   Number of Packets    Number of Bytes

Green                        0                  0
Yellow                       0                  0
Red                          0                  0


FUF statistics:
Drop count: 0
```

Collecting Statistics on Gates with Rate-Limited Flows

When fast update filters (FUF) are installed on the Packet Forwarding Engine and PIC, the Packet Forwarding Engine and PIC discard packets flowing through gates if they exceed the rate limits set in the FUF. To get accurate statistics for gates, the JUNOS Software includes these discarded packets in statistics that it collects for gates.

Improving Performance While Collecting Gate Statistics

Collecting statistics on packets that are dropped on a gate can impact system performance. To improve performance, the software can limit the number of FUF terms installed on the Packet Forwarding Engine for a virtual BGF. This limit is the maximum value of the following parameters configured on the router:

- The maximum number of FUF terms installed for the virtual BGF
- The maximum percentage of gates with FUF filters relative to all gates currently installed for the virtual BGF

Step-by-Step Procedure To configure a limit on the number of FUF terms installed on the Packet Forwarding Engine for a virtual BGF:

1. Access the configuration of your virtual BGF.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1
   ```

2. Specify the maximum number of FUF terms installed for the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set fast-update-filter maximum-terms 3000
   ```

3. Specify the maximum percentage of gates with FUF filters relative to all gates currently installed for the virtual BGF.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#set fast-update-filter maximum-fuf-percentage 15
   ```

Displaying the Number of FUF Terms Installed on a Virtual BGF

Purpose Display the number of match condition FUF terms and the number of FUF filters currently installed on a virtual BGF using the show services pgcp active-configuration gateway *gateway-name* command.

Action

```
user@host> show services pgcp active-configuration gateway bgf-1
. . .
Firewall:
  Status             :  Connected
  Number of terms    :  2
  Number of filters  :  2
```

Displaying Gates That Are Being Mirrored

You can view session mirroring information for gates that are being mirrored. You must have a login with sufficient permission to view session mirroring information. The set system login class *class-name* permissions pgcp-session-mirroring command grants this permission.

Purpose Display session-mirroring information for a gate using the show services pgcp gate gateway *gateway-name* gate-id *gate-id* session-mirroring command.

Action

```
user@host> show services pgcp gate gateway bgf-1 gate-id 4295033088
session-mirroring

Gate information:
Gate id: 4295033088
Session mirroring status: On
Session mirroring correlation number: 0x8040c020a060e010
Session mirroring target ID list: [008040c0, ffffff80]
Session mirroring direction: Egress
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Monitoring Terminations

To monitor terminations, you can display the following information on the router:

Displaying Information About All Terminations on a Virtual BGF

Purpose Display information about all terminations on a virtual BGF using the show services pgcp terminations gateway *gateway-name* command.

Action

```
user@host> show services pgcp terminations gateway bgf-1
Virtual BGF configuration:
  Name                                  :  bgf-1
  IP address                            :  2.0.0.2
  Port                                  :  2944
  Status                                :  In-Service (Registered)


Termination name                   State           Duration(msecs)
ip/4/vif-0/3                       In-service      920610
Gate-id         Direction       State        Action
4295033088      A->B            active       forward
4295033089      B->A            active       forward


Termination name                   State           Duration(msecs)
ip/4/vif-0/2                       In-service      920618
Gate-id         Direction       State        Action
4295033088      A->B            active       forward
4295033089      B->A            active       forward
```

Displaying Information About Terminations in H.248 Format

Purpose Display information about terminations in H.248 format using the show services pgcp terminations gateway *gateway-name* h248 command.

Action

```
user@host> show services pgcp terminations gateway bgf-1 h248
Termination information:
ip/4/vif-0/2 {

      MEDIA {

        TERMINATIONSTATE { SERVICESTATES = INSERVICE },

        STREAM = 1 {

          LOCALCONTROL { MODE = SENDRECEIVE,

                         DS/DSCP = 00,

                         TMAN/MBS = 5000,

                         TMAN/PDR = 0,

                         TMAN/POL = ON,

                         TMAN/SDR = 125000,

                         MGCINFO/DB = 00,

                         GM/RSB = OFF,

                         GM/SAF = OFF,

                         GM/SPF = OFF,

                         GM/SPR = 0,

                         GM/ESAS = OFF,

                         GM/ESPS = OFF,

                         GM/LSP = 0 },

          LOCAL {

v=0

c=IN IP4 4.99.99.20

m=- 5060 udp -

b=AS:0


          },

          REMOTE {

v=0

c=IN IP4 4.0.0.1

m=- 5060 udp -

b=AS:0
```

```
          }
        }
      },
      EVENTS { HANGTERM/THB { TIMERX= 30 } }
}
ip/4/vif-0/3 {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = INSERVICE },
        STREAM = 1 {
          LOCALCONTROL { MODE = SENDRECEIVE,
                         DS/DSCP = 00,
                         TMAN/MBS = 5000,
                         TMAN/PDR = 0,
                         TMAN/POL = ON,
                         TMAN/SDR = 125000,
                         MGCINFO/DB = 00,
                         GM/RSB = OFF,
                         GM/SAF = OFF,
                         GM/SPF = OFF,
                         GM/SPR = 0,
                         GM/ESAS = OFF,
                         GM/ESPS = OFF,
                         GM/LSP = 0 },
          LOCAL {
v=0
c=IN IP4 2.99.99.20
m=- 5060 udp -
b=AS:0
          },
```

```
          REMOTE {
v=0
c=IN IP4 2.0.0.1
m=- 5060 udp -
b=AS:0

          }
        }
      },
      EVENTS { HANGTERM/THB { TIMERX= 30 } }

 }
```

Displaying Information About Specific Terminations

Purpose Display information about a specific termination using the show services pgcp terminations gateway *gateway-name* termination-prefix *termination-prefix* h248 command. For the termination prefix, you can enter a partial name, and all matching terminations are displayed.

Action

```
user@host> show services pgcp terminations gateway bgf-1 termination-prefix
ip/4/vif-0/3 h248
Termination information:
ip/4/vif-0/3 {

      MEDIA {

        TERMINATIONSTATE { SERVICESTATES = INSERVICE },

        STREAM = 1 {

          LOCALCONTROL { MODE = SENDRECEIVE,

                         DS/DSCP = 00,

                         TMAN/MBS = 5000,

                         TMAN/PDR = 0,

                         TMAN/POL = ON,

                         TMAN/SDR = 125000,

                         MGCINFO/DB = 00,

                         GM/RSB = OFF,

                         GM/SAF = OFF,

                         GM/SPF = OFF,
```

```
                              GM/SPR = 0,
                              GM/ESAS = OFF,
                              GM/ESPS = OFF,
                              GM/LSP = 0 },
                LOCAL {
v=0
c=IN IP4 4.99.99.20
m=- 5060 udp -
b=AS:0

                },
                REMOTE {
v=0
c=IN IP4 4.0.0.1
m=- 5060 udp -
b=AS:0

                }
              }
            },
            EVENTS { HANGTERM/THB { TIMERX= 30 } }
}
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Monitoring PGCP Root Terminations

Purpose Display information about the root termination on a virtual BGF using the show services pgcp root-termination gateway *gateway-name* command.

Action

```
user@host> show services pgcp root-termination gateway bgf-1
Root termination information:
ROOT {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = OUTOFSERVICE,
```

```
                                    ROOT/MAXNUMBEROFCONTEXTS = 21000,
                                    ROOT/MAXTERMINATIONSPERCONTEXT = 2,
                                    ROOT/MGCORIGINATEDPENDINGLIMIT = 4,
                                    ROOT/MGCPROVISIONALRESPONSETIMERVALUE = 4000,
                                    ROOT/MGORIGINATEDPENDINGLIMIT = 4,
                                    ROOT/MGPROVISIONALRESPONSETIMERVALUE = 2000,
                                    ROOT/NORMALMGCEXECUTIONTIME = 500,
                                    ROOT/NORMALMGEXECUTIONTIME = 500,
                                    SEG/MGCMAXPDUSIZE = 1472,
                                    SEG/MGCSEGMENTATIONTIMERVALUE = 4000,
                                    SEG/MGMAXPDUSIZE = 1472,
                                    SEG/MGSEGMENTATIONTIMERVALUE = 4000 }
                  },
                  EVENTS = 3 { IT/ITO { MIT = 12000 } }
                }
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Monitoring Statistics for the Virtual BGF

You can monitor statistics for the virtual BGF with the show services pgcp statistics gateway *gateway-name* command. You can include the extensive keyword to display additional information.

Purpose Display statistics for H.248 messages, protocol errors, and commands using the show services pgcp statistics gateway *gateway-name* extensive command.

Action

```
user@host> show services pgcp statistics gateway bgf-1 extensive
Virtual BGF configuration:
  Name                                  :  pg1
  IP address                            :  10.50.150.100
  Port                                  :  2944
  Status                                :  In-Service (Registered)

H.248 statistics:
    Messages received          :  5
    Messages sent              :  3
    Protocol errors            :  0

Received Commands        Total          Wildcard        Success          Error
```

```
    Add                 0             0             0             0
    AuditValue          1             0             1             0
    Modify              1             0             1             0
    ServiceChange       0             0             0             0
    Subtract            0             0             0             0

Sent Commands           Total         Wildcard      Success       Error

    Notify              0             0             0             0
    ServiceChange       1             0             1             0

ROOT SVC                Total         Wildcard      Success       Error

    DC/900              0             0             0             0
    FL/908              0             0             0             0
    FL/909              0             0             0             0
    FL/919              0             0             0             0
    FL/920              0             0             0             0
    FO/904              0             0             0             0
    FO/905              0             0             0             0
    FO/908              0             0             0             0
    GR/905              0             0             0             0
    HO/903              0             0             0             0
    RS/900              0             0             0             0
    RS/901              1             0             1             0
    RS/902              0             0             0             0
    RS/918              0             0             0             0

Termination SVC         Total         Wildcard      Success       Error

    FO/904              0             0             0             0
    FO/905              0             0             0             0
    FO/906              0             0             0             0
    FO/907              0             0             0             0
    FO/910              0             0             0             0
    FO/915              0             0             0             0
    GR/905              0             0             0             0
    RS/900              0             0             0             0
    RS/918              0             0             0             0

ROOT Notify             Total         Wildcard      Success       Error

    ocp/mg_overloaded   0             0             0             0

Termination Notify      Total         Wildcard      Success       Error

    adid/ipstop         0             0             0             0
    nt/qualert          0             0             0             0
    adr/rtac            0             0             0             0
    hangterm/thb        0             0             0             0
```

Meaning There is no relationship between the messages received and sent counters and the command request and response counters. The message counters describe the network activity and contain all H.248 messages. Each message can contain one or more commands, and commands that contain wildcards can be interpreted as more than one command.

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Monitoring Flows

You can view flows with the show services pgcp flows gateway *gateway-name* command. You can view information for all flows, or you can include keywords to limit the number of flows displayed or to display flows for a particular:

- Gate
- Source or destination port
- Source or destination prefix
- Source or destination routing instance
- Protocol
- Service set

Displaying All Flows

Purpose Display standard information about all flows using the show services pgcp flows gateway *gateway-name* command.

Action

```
user@host> show services pgcp flows gateway bgf-1
Interface: sp-0/3/0, Service set: bgf-svc-set-1
Flow                                                 State    Dir       Frm count
UDP          4.0.0.102:0     ->    4.99.99.100:1024  Forward  I           21531
Gate id: 8590000385
    NAT source       4.0.0.102:0       ->     3.99.99.100:1024
    NAT dest       4.99.99.100:1024    ->       3.0.0.101:49174
UDP            0.0.0.0:0     ->    3.99.99.100:1024  Forward  I           20999
Gate id: 8590000384
    NAT source         0.0.0.0:0       ->     4.99.99.100:1024
    NAT dest       3.99.99.100:1024    ->       4.0.0.102:49234
UDP          4.0.0.102:0     ->    4.99.99.100:5060  Forward  I               3
Gate id: 4295033089
    NAT source       4.0.0.102:0       ->     3.99.99.100:5060
    NAT dest       4.99.99.100:5060    ->       3.0.0.101:5060
UDP          3.0.0.101:0     ->    3.99.99.100:5060  Forward  I               2
Gate id: 4295033088
    NAT source       3.0.0.101:0       ->     4.99.99.100:5060
    NAT dest       3.99.99.100:5060    ->       4.0.0.102:5060
UDP            0.0.0.0:0     ->    3.99.99.100:1025  Forward  I               0
Gate id: 8590000384
    NAT source         0.0.0.0:0       ->     4.99.99.100:1025
    NAT dest       3.99.99.100:1025    ->       4.0.0.102:49235
UDP          4.0.0.102:0     ->    4.99.99.100:1025  Forward  I               0
Gate id: 8590000385
    NAT source       4.0.0.102:0       ->     3.99.99.100:1025
    NAT dest       4.99.99.100:1025    ->       3.0.0.101:49175
```

Displaying Extensive Information About All Flows

Purpose Display extensive information about all flows, using the show services pgcp flows gateway *gateway-name* extensive command.

Action

```
user@host> show services pgcp flows gateway bgf-1 extensive
Interface: sp-1/2/0, Service set: bgf-svc-set
Flow                                                State    Dir       Frm count
Gate id: 4295033088
UDP                :::0     ->  222::99:99:20:5060  Forward  I              0
    NAT source             :::0       ->     4::99:99:20:5060
    NAT dest     222::99:99:20:5060    ->        4::1:1:3:5060
  Byte count: 0
  Flow role: Master, Timeout: 429496728
  Tman Policing: ON
  SDR    : 10000 bytes per second
  SDR MBS: 1000 bytes
  PDR    : 10000 bytes per second
  PDR MBS: 1000 bytes
Gate id: 4295033088
UDP                :::0     ->    4::99:99:20:5060  Forward  I              0
    NAT source             :::0       ->   222::99:99:20:5060
    NAT dest       4::99:99:20:5060    ->          222::6:5060
  Byte count: 0
  Flow role: Responder, Timeout: 429496728
  Tman Policing: ON
  SDR    : 500 bytes per second
  SDR MBS: 1000 bytes
  PDR    : 500 bytes per second
  PDR MBS: 1000 bytes
```

Displaying Extensive Information About Flows for a Specific Gate

Purpose Display extensive information about flows for a specific gate using the show services pgcp flows gateway *gateway-name* gate-id *gate-id* extensive command.

Action

```
user@host> show services pgcp flows gateway bgf-1 gate-id 4295033088 extensive
Interface: rsp1, Service set: bgf-svc-set-1
Flow                                                State    Dir       Frm count
Gate id: 4295033088
UDP          4.0.0.102:0     ->    10.50.100.1:1024  Forward  I              0
    NAT source       4.0.0.102:0       ->     20.50.100.1:1024
    NAT dest       10.50.100.1:1024    ->       4.0.0.101:10000
  Byte count: 0
  Flow role: Master, Timeout: 429496728
  Tman Policing: ON
  SDR    : 10000 bytes per second
  SDR MBS: 1000 bytes
  PDR    : 10000 bytes per second
  PDR MBS: 1000 bytes
Gate id: 4295033088
UDP          4.0.0.102:0     ->    10.50.100.1:1025  Forward  I              0
    NAT source       4.0.0.102:0       ->     20.50.100.1:1025
    NAT dest       10.50.100.1:1025    ->       4.0.0.101:10001
  Byte count: 0
  Flow role: Initiator, Timeout: 429496728
  Tman Policing: ON
```

```
SDR    : 500 bytes per second
SDR MBS: 1000 bytes
PDR    : 500 bytes per second
PDR MBS: 1000 bytes
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Monitoring Conversations

A conversation is a group of flows that are grouped based on the call that they belong to. A voice call typically has four flows—an RTP and an RTCP flow in the forward direction, and an RTP and an RTCP flow in the reverse direction. If the gateway controller does not create RTCP flows, the call has two flows—an RTP flow in each direction.

You can view conversations with the show services pgcp conversations gateway *gateway-name* command. You can view information for all conversations, or you can include keywords to limit the number of conversations displayed or to display conversations for a particular:

- Source or destination port
- Source or destination prefix
- Source or destination routing instance
- Protocol
- Service set

Displaying All Conversations

Purpose Display standard information about all conversations using the show services pgcp conversations gateway *gateway-name* command.

Action

```
user@host> show services pgcp conversations gateway bgf-1
Interface: sp-0/3/0, Service set: bgf-svc-set-1

Conversation: ALG protocol: any
  Number of initiators: 2, Number of responders: 2
Flow                                                State    Dir       Frm count
UDP          4.0.0.102:0     ->    4.99.99.100:1024  Forward  I           20051
Gate id: 8590000385
    NAT source       4.0.0.102:0       ->     3.99.99.100:1024
    NAT dest       4.99.99.100:1024    ->       3.0.0.101:49174
UDP          4.0.0.102:0     ->    4.99.99.100:1025  Forward  I               0
Gate id: 8590000385
    NAT source       4.0.0.102:0       ->     3.99.99.100:1025
    NAT dest       4.99.99.100:1025    ->       3.0.0.101:49175
UDP            0.0.0.0:0     ->    3.99.99.100:1024  Forward  I           19551
Gate id: 8590000384
    NAT source         0.0.0.0:0       ->     4.99.99.100:1024
    NAT dest       3.99.99.100:1024    ->       4.0.0.102:49234
UDP            0.0.0.0:0     ->    3.99.99.100:1025  Forward  I               0
Gate id: 8590000384
```

```
    NAT source         0.0.0.0:0       ->     4.99.99.100:1025
    NAT dest       3.99.99.100:1025    ->       4.0.0.102:49235

Conversation: ALG protocol: any
  Number of initiators: 1, Number of responders: 1
Flow                                                State    Dir       Frm count
UDP          3.0.0.101:0     ->    3.99.99.100:5060  Forward  I              2
Gate id: 4295033088
    NAT source       3.0.0.101:0       ->     4.99.99.100:5060
    NAT dest       3.99.99.100:5060    ->       4.0.0.102:5060
UDP          4.0.0.102:0     ->    4.99.99.100:5060  Forward  I              3
Gate id: 4295033089
    NAT source       4.0.0.102:0       ->     3.99.99.100:5060
    NAT dest       4.99.99.100:5060    ->       3.0.0.101:5060
```

Displaying Extensive Information About All Conversations

Purpose Display extensive information about all conversations using the show services pgcp conversations gateway *gateway-name* extensive command.

Action

```
user@host> show services pgcp conversations gateway bgf-1 extensive
Interface: sp-1/2/0, Service set: bgf-svc-set

Conversation: ALG protocol: any
  Number of initiators: 1, Number of responders: 1
Flow                                                State    Dir       Frm count
Gate id: 4295033088
UDP                :::0     ->  222::99:99:20:5060  Forward  I              0
    NAT source             :::0       ->     4::99:99:20:5060
    NAT dest     222::99:99:20:5060    ->        4::1:1:3:5060
  Byte count: 0
  Flow role: Master, Timeout: 429496728
  Tman Policing: ON
  SDR    : 10000 bytes per second
  SDR MBS: 1000 bytes
  PDR    : 10000 bytes per second
  PDR MBS: 1000 bytes
Gate id: 4295033088
UDP                :::0     ->    4::99:99:20:5060  Forward  I              0
    NAT source             :::0       ->   222::99:99:20:5060
    NAT dest       4::99:99:20:5060    ->          222::6:5060
  Byte count: 0
  Flow role: Responder, Timeout: 429496728
  Tman Policing: ON
  SDR    : 500 bytes per second
  SDR MBS: 1000 bytes
  PDR    : 500 bytes per second
  PDR MBS: 1000 bytes
```

Related Topics

- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Chapter 6

Managing the BGF

This chapter describes how to manage the pgcpd process and how to shut down virtual BGFs and virtual interfaces. Topics include:

Managing the pgcpd Process Running on the Routing Engine

You can stop and start the pgcpd process that is running on the Routing Engine in any of these ways:

- Restart the pgcpd process. In this procedure, the pgcpd process is considered configured.
- Disable and enable the pgcpd process. In this procedure, the pgcpd process is considered configured.
- Activate and deactivate the PGCP service.

The gateway controller cannot send add, modify, or subtract commands to the pgcpd process.

Restarting the pgcpd Process Running on the Routing Engine

CAUTION: We recommend that you do not restart the software process unless instructed to do so by a Juniper Networks customer support engineer. A restart might cause the router to drop calls and interrupt transmission.

Three options are available when you restart the pgcpd process that is running on the Routing Engine:

- gracefully—Restart the software process after calls have ended.
- immediately—Immediately restart the software process.
- soft— Reread and reactivate the configuration without completely restarting the software process.

To restart the pgcpd process, enter the restart pgcp-service command in operational mode:

```
user@host>restart pgcp-service immediately
```

When you restart the pgcpd process, the process is stopped and then restarted.

Disabling and Enabling the pgcpd Process

This topic describes the process of disabling and enabling the pgcpd process. You can disable and enable the pgcpd process only on the Routing Engine. You cannot disable or enable pgcpd processes running on MultiServices PICs.

Disabling the pgcpd Process

To disable the pgcpd process, enter the set system processes pgcp-service disable statement in configuration mode, and then commit your configuration:

```
user@host# set system processes pgcp-service disable
user@host# commit
```

Enabling the pgcpd Process

To enable the pgcpd process, enter the delete system processes pgcp-service disable statement in configuration mode, and then commit your configuration:

```
user@host# delete system processes pgcp-service disable
user@host# commit
```

Activating and Deactivating PGCP Services Running on the Routing Engine

This topic describes the process of deactivating and activating the PGCP service.

Deactivating the PGCP Service

To deactivate the PGCP service, enter the deactivate services pgcp statement in configuration mode:

```
user@host# deactivate services pgcp
```

The Routing Engine is stopped and the PGCP configuration is removed from the router.

Activating the PGCP Service

The PGCP service is activated by default. If you have deactivated the service, you can activate it by entering the activate services pgcp statement in configuration mode:

```
user@host# activate services pgcp
```

Managing the pgcpd Process Running on a Services PIC

You can stop and start the pgcpd process that is running on a services PIC in any of these ways:

- Restart the pgcpd process.
- Activate and deactivate the PGCP service.

Restarting the pgcpd Process Running on a Services PIC

CAUTION: We recommend that you do not restart the software process unless instructed to do so by a Juniper Networks customer support engineer. A restart might cause the router to drop calls and interrupt transmission.

To restart the process of a specific virtual BGF running on a services PIC, enter the restart services pgcp gateway *gateway-name* command in operational mode:

```
user@host>restart services pgcp gateway bgf-1
```

This command causes the router to send a service-change command to the gateway controller for all virtual BGFs running on the process, not just the virtual BGF that you specified when you entered the restart command.

Activating and Deactivating PGCP Services Running on a Services PIC

This topic describes the process of deactivating and activating the PGCP service.

Deactivating the PGCP Service

To deactivate the PGCP service, enter the deactivate services pgcp statement in configuration mode:

```
user@host# deactivate services pgcp
```

The services PIC is stopped, but the configuration is not removed from the router.

Activating the PGCP Service

The PGCP service is activated by default. If you have deactivated the service, you can activate it by entering the activate services pgcp statement in configuration mode:

```
user@host# activate services pgcp
```

Shutting Down a Virtual BGF

You can shut down the virtual BGF in two ways—forced or graceful:

- Forced—The virtual BGF immediately removes all gates and disconnects from the gateway controller. The virtual BGF does not attempt to establish a new connection.
- Graceful—The virtual BGF goes out of service by entering a draining mode and waiting for all terminations to be subtracted before going out of service. During the draining, the virtual BGF accepts only subtract and audit commands from the gateway controller.

Forcing the Shutdown of a Virtual BGF

To perform a forced shutdown of the virtual BGF, enter set service-state out-of-service-forced at the [edit services pgcp gateway *gateway-name*] hierarchy level. For example:

```
[edit services pgcp gateway bgf-1]
user@host#set service-state out-of-service-forced
```

Performing a Graceful Shutdown of a Virtual BGF

To perform a graceful shutdown of the virtual BGF, enter set service-state out-of-service-graceful at the [edit services pgcp gateway *gateway-name*] hierarchy level. For example:

```
[edit services pgcp gateway bgf-1]
user@host#set service-state out-of-service-graceful
```

Making the Virtual BGF Operational Again

To cause the virtual BGF to be operational again and available for traffic, set the service state to in-service with the set service-state in-service statement. When the virtual BGF is in service, it attempts to connect to the gateway controller and accepts all PGCP commands from the gateway controller. For example:

```
[edit services pgcp gateway bgf-1]
user@host#set service-state in-service
```

Shutting Down a Virtual Interface

Shutting down the virtual interface is useful when you do not want to shut down the entire virtual BGF. You can shut down the virtual interface two ways—forced or graceful:

- Forced—The virtual interface immediately removes all calls and disconnects from the physical interface.

- Graceful—The virtual interface goes out of service by entering a draining mode and waiting for all terminations to be subtracted before going out of service. During the draining, terminations associated with the virtual interface accept only subtract commands from the gateway controller.

Forcing the Shutdown of a Virtual Interface

To perform a forced shutdown of a virtual interface, enter set service-state out-of-service-forced at the [edit services pgcp virtual-interface *interface-number*] hierarchy level. For example:

```
[edit services pgcp virtual-interface 1]
user@host#set service-state out-of-service-forced
```

Performing a Graceful Shutdown of a Virtual Interface

To perform a graceful shutdown of a virtual interface, enter set service-state out-of-service-graceful at the [edit services pgcp virtual-interface *interface-number*] hierarchy level. For example:

```
[edit services pgcp virtual-interface 1]
user@host#set service-state out-of-service-graceful
```

Making the Virtual Interface Operational Again

To cause the virtual interface to be operational again and available for traffic, set the service state to in-service with the set service-state in-service statement. When the virtual interface is in service, it is connected to the physical interface and accepts all voice calls. For example:

```
[edit services pgcp virtual-interface 1]
user@host#set service-state in-service
```

Maintaining Synchronization Between the BGF and the Gateway Controller

The BGF software uses the following features to maintain synchronization between the BGF and the gateway controller.

- Detecting Hanging Terminations on page 117
- Detecting Gateway Controller Failures on page 119
- Maintaining Synchronization by Auditing Terminations on page 120

Detecting Hanging Terminations

Synchronization of termination information between the BGF and the gateway controller is essential for traffic, maintenance, and charging purposes. If a termination does not exchange messages for a period of time, corresponding data for the termination might be mismatched on the BGF and the gateway controller, and the termination can be hanging. Hanging terminations can consume resources that can be used for chargeable calls.

To detect possible hanging terminations, the BGF uses a timer that begins when a message is exchanged for a specific termination. If the termination does not receive a message when the timer expires, the BGF notifies the gateway controller. If the data on the gateway controller does not match the data on the BGF, the gateway controller returns one of the following error messages to the BGF:

```
Error Code #: 411 Name: The transaction refers to an unknown ContextID
Error Code #: 430 Name: Unknown TerminationID
Error Code #: 435 Name: Termination ID is not in specified Context
```

The gateway controller is responsible for correcting mismatches in data. For example, the gateway controller can subtract the indicated termination and clear associated contexts. The gateway controller can also audit the termination service state to check its records before taking further action.

Activating and Configuring Hanging Termination Detection

The timerx timer sets the interval between the last message exchanged for a specific termination and when the BGF sends a notification to the gateway controller. The timer resets when a message is exchanged on the termination and when the BGF notifies the gateway controller. For example, if the BGF notifies the gateway controller that there has been no activity on the termination, and the gateway controller does not modify or subtract the indicated termination, the BGF again waits the specified time, and sends another notification if there still has not been activity on the termination.

Setting the timer to a value other than zero (0) activates hanging termination detection on new and modified terminations. The timer value that you set is the default value, and it can be overridden by H.248 messages sent from the gateway controller. To set the timer:

```
[edit services pgcp gateway bgf-1 h248-properties hanging-termination-detection]
user@host#set timerx 30
```

Deactivating Hanging Termination Detection

To deactivate hanging termination detection, set the timerx statement to 0:

```
[edit services pgcp gateway bgf-1 h248-properties hanging-termination-detection]
user@host#set timerx 0
```

Displaying the Value of the Timerx Timer Configured on the Virtual BGF

Purpose Display the value of the timerx that is configured on the virtual BGF

Action

```
[edit services pgcp gateway bgf-1 h248-properties hanging-termination-detection]
user@host# show
timerx 30;
```

Displaying the Value of the Hanging Termination Timer for a Termination

Purpose Display the timerx value for a termination.

Action

```
user@host> show services pgcp terminations gateway bgf-1 h248
Termination information:
ip/4/vif-0/2 {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = INSERVICE },
        STREAM = 1 {
          LOCALCONTROL { MODE = SENDRECEIVE, GM/LSP = 0 },
           LOCAL {
            v = 0,
            c=IN IP4 10.50.100.1
            m=- 1080 RTP/AVP  –
            b=AS:0
          }
        }
      }
      EVENTS { HANGTERM/THB { TIMERX = 30 } }
}
```

Detecting Gateway Controller Failures

The BGF supports the inactivity timer package defined in *Gateway control protocol: Inactivity timer package H.248.14, March 2002*. This feature allows the BGF to detect the failure of its active gateway controller through message inactivity. The inactivity timer is applied to the root terminations of a virtual BGF.

The inactivity timer package specifies a default maximum inactivity time. This timer resets each time the BGF receives a message from the gateway controller. If the BGF does not receive a message from the gateway controller before the maximum inactivity time expires, it sends a Notify message with the observed inactivity timeout event to the gateway controller. If the gateway controller does not reply to the message, the BGF considers the gateway controller as failed.

Configuring the Inactivity Timer Package

Step-by-Step Procedure

To configure the inactivity timer package:

1. Access the inactivity timeout configuration for a virtual BGF.

   ```
   [edit services pgcp]
   user@host#edit gateway bgf-1 h248-properties inactivity-timer inactivity-timeout
   ```

2. Specify whether the BGF detects inactivity timeout events received from the gateway controller by default.

   ```
   [edit services pgcp gateway bgf-1 h248-properties inactivity-timer inactivity-timeout]
   user@host#set detect
   ```

3. Specify a default value for the maximum inactivity time. The default value is used if the gateway controller requests that the BGF detect the inactivity timeout event, but the gateway controller does not set a value for the maximum inactivity time.

   ```
   [edit services pgcp gateway bgf-1 h248-properties inactivity-timer inactivity-timeout]
   user@host#set maximum-inactivity-time default 24000
   ```

Maintaining Synchronization by Auditing Terminations

You can use the AuditValue command in H.248 messages to maintain synchronization between the BGF and the gateway controller. The AuditValue command requests the current values of a descriptor or of a single property, event, signal, or statistic associated with terminations and contexts. You can include selection criteria in the AuditValue command to filter the returned values.

The software supports the following characters for audit selection criteria:

- equal to (=)
- not equal to (#)
- less than (<)
- greater than (>)

Using AND/OR Logic with Audit Commands

You can include multiple criteria with an AND or an OR logic operation (ANDLgc, ORLgc) to indicate how the selection criteria are interpreted. If you do not include a logic operation, AND logic operation is applied.

Example: Audit Section Filter with AND Logic

Purpose Create an audit selection filter for contexts and terminations that have the saf property set to on AND the spr property set to less than 4075.

Action

```
Transaction = 201 {
    Context = * {
        ContextAudit {
            ANDLgc
        },
        AuditValue = * {
            Audit {
                Media {
                    LocalControl {
                        gm/saf=on,
                        gm/spr<4075,
                    }
                }
            }
        }
    }
}
```

Meaning The result of this audit is a list of terminations that have the saf property set to on and the spr property set to less than 4075.

Example: Audit Section Filter with OR Logic

Purpose Create an audit selection filter for contexts and terminations that have the spf property set to on OR the sam property set to 10.10.0.3.

Action

```
Transaction = 202 {
    Context = * {
        ContextAudit {
            ORLgc
        },
        AuditValue = * {
            Audit {
                Media {
                    LocalControl {
                        gm/spf=on,
                        gm/sam=10.10.0.3,
                    }
                }
            }
        }
    }
}
```

Meaning The result of this audit is a list of terminations that have the spf property set to on or the sam property set to 10.10.0.3.

Managing Overload Control with Priority Handling for Emergency Calls

You can enable the virtual BGF to notify a gateway controller when it experiences processing overload that might prevent the timely execution of H.248 transactions. The gateway controller can then adjust how H.248 transactions are passed to the virtual BGF. The configurable overload control options provide priority handling for emergency calls.

The gateway controller activates the overload control feature by setting the overload control event. Incoming H.248 transactions are pushed into a work queue. Overload control actions are based on the following user-defined threshold levels:

- queue-limit-percentage—When the pending transactions in the work queue occupy this percentage of the maximum queue size, the virtual BGF sends an overload notification for each received ADD command in incoming H.248 transactions. The gateway controller lowers the rate used to admit calls to the virtual BGF (the admitted rate). The actions to be initiated for each overload threshold are configured on the gateway controller.
- reject-new-calls-threshold—When this threshold is reached, the virtual BGF rejects all non-emergency ADD transactions. Emergency ADD transactions, SUBTRACT, MODIFY, and AUDIT transactions are admitted. This percentage must be greater than or equal to the percentage specified for queue-limit-percentage.
- reject-all-commands-threshold—When this threshold is reached, all non-emergency transactions except for SUBTRACT transactions are rejected. This percentage must be greater than or equal to the percentage specified for reject-new-calls-threshold.

When transactions in the work queue occupy 100 percent of the work queue's maximum size, the virtual BGF drops received transactions and sends error code #511 (Temporarily Busy). When transactions in the work queue occupy less than the queue-limit-percentage, overload notifications are no longer sent.

Configuring Overload Control for Voice Calls

You configure overload control by configuring the queue limit percentage, the threshold for rejecting non-emergency new calls, and the threshold for rejecting all non-emergency transactions except for SUBTRACT transactions. When you configure overload control for the BGF, you must set the reject-new-calls-threshold to a value greater than or equal to the queue-limit-percentage, and you must set the reject-all-commands-threshold to a value greater than or equal to the reject-new-calls-threshold.

Step-by-Step Procedure To configure overload-control for voice calls:

1. Access the configuration of overload control.

   ```
   [edit services pgcp gateway bgf-1]
   user@host#edit overload-control
   ```

2. Configure a queue limit percentage.

   ```
   [edit services pgcp gateway bgf-1 overload-control]
   user@host#set queue-limit-percentage 70
   ```

3. Configure a threshold for rejecting all non-emergency new calls.

   ```
   [edit services pgcp gateway bgf-1 overload-control]
   user@host#set reject-new-calls-threshold 80
   ```

4. Configure a threshold for rejecting all non-emergency new transactions except SUBTRACT transactions.

   ```
   [edit services pgcp gateway bgf-1 overload-control]
   user@host#set reject-all-command-threshold 90
   ```

NOTE: Only one work queue exists for the entire device. The queue limit percentage that you configure applies to the entire device, not just the virtual BGF named in the hierarchy level you have chosen. If you enter multiple queue limit percentages for different virtual BGFs, only the last entry is used.

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Preventing Excessive Media Inactivity Notifications

You can prevent a BGF from sending an excessive number, or *avalanche*, of media inactivity notifications to the gateway controller in a short period of time. Such an avalanche can severely degrade the performance of the gateway controller. By default, all media inactivity notifications are sent immediately from the BGF to the gateway controller. When an upstream device in the network fails, all existing terminations in the BGF report media inactivity at about the same time. You can configure H.248

notification behavior to regulate the flow of notifications sent to the gateway controller.

Regulated notification is activated either by a request from the gateway controller or by CLI commands. When you choose regulated notification you can explicitly configure the frequency for notifications of media inactivity events as follows:

- Send only one media inactivity notification. This option is not available as part of the H.248 notification behavior package.
- Send a configurable percentage of media inactivity notifications (0 through 100).

Notification History—The Notification Behavior Package only limits the sending of notifications to the gateway controller, not the occurrences of the event. We recommend you enable the recording of all media inactivity notifications for future retrieval and, optionally, request that the inactivity notifications time stamps are also enabled for future retrieval.

Configuring H.248 Notification Behavior to Prevent Excessive Media Inactivity Notifications

By properly setting H.248 notification behavior properties, you can prevent a BGF from sending an avalanche of media inactivity notifications that can flood the gateway controller and adversely affect the processing of H.248 transactions. You can also enable recording of all media inactivity events for future retrieval.

The H.248 Notification Behavior package is defined in annex E.15 of the *Gateway control protocol v.3, ITU-T Recommendation H.248.1, September, 2005*.

Step-by-Step Procedure To configure default values for H.248 Notification Behavior properties:

1. Access the configuration of H.248 application-data-inactivity-detection.

```
[edit services pgcp gateway bgf-1]
user@host#edit h248-properties application-data-inactivity-detection
```

2. Turn notification on.

```
[edit services pgcp gateway bgf-1 h248-properties
   application-data-inactivity-detection]
user@host#set ip-flow-stop-detection regulated-notify
```

3. Access the configuration of H.248 notification behavior.

```
[edit services pgcp gateway bgf-1]
user@host#edit h248-properties notification-behavior
```

4. Configure the default frequency of notification messages for the media inactivity event. The gateway controller can override this default by requesting a different frequency. If you specify **once**, only one notification is sent and the gateway controller cannot retrieve the notification by use of an audit for the root.termination.

```
[edit services pgcp gateway bgf-1 h248-properties notification-behavior]
user@host#set notification-regulation default 10
```

5. Enable retrieval of event notifications by the gateway controller at the [edit services pgcp gateway *gateway-name* h248-options] level.

```
[edit services pgcp gateway bgf-1 h248-properties notification-behavior]
user@host#up 2
[edit services pgcp gateway bgf-1]
user@host#edit h248–options
[edit services pgcp gateway bgf-1 h248-options]
user@host#set audit-observed-events-returns-history;
```

6. Enable retrieval of time stamps of recorded notifications by the gateway controller.

```
[edit services pgcp gateway bgf-1 h248-options]
user@host#edit services pgcp gateway bgf-1 h248-properties
[edit services pgcp gateway bgf-1 h248-properties]
user@host#set event-timestamp-notification request-timestamp requested
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Managing the Rate for All Notifications Sent by a PIC or DPC

You can limit the rate at which the PIC or DPC sends all notifications. Using this functionality, you can prevent an avalanche of media inactivity notifications and throttle all notifications to a configured rate. Doing this enables the system to maintain a stable state when the PIC or DPC is generating a large volume of messages.

Limiting the Rate for All Notifications from a PIC or DPC

You can configure the aggregate rate of notifications coming from a PIC or DPC. Using this approach, you limit the rate for all messages from the PIC or DPC, not just notifications.

Step-by-Step Procedure

To configure a rate limit for a PIC or DPC to send notifications to the gateway controller:

1. Access the configuration of PGCP parameters.

```
[edit services]
user@host#edit pgcp
```

2. Configure the rate (per second) for PICs to send messages to the gateway controller.

```
[edit services pgcp ]
user@host#set notification-rate-limit 25
```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Enabling Wildcards for ServiceChange Notifications

You can enable the virtual BGF to issue ServiceChange commands as wildcard-response commands, which trigger a short response from the gateway controller. If you do not enable the use of wildcard response for ServiceChange commands, the gateway controller generates an individual response for every termination that matches the ServiceChange command.

Step-by-Step Procedure

To enable wildcard-response commands for ServiceChange commands:

1. Access the service change configuration.

```
[edit services pgcp gateway bgf-1]
user@host#edit h248-options service-change
```

2. Enable the virtual BGF to issue ServiceChange commands as wildcard-response commands.

```
[edit services pgcp gateway bgf-1 h248-options service-change]
user@host#set use-wildcard-response
```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Controlling ServiceChange Commands Sent from the Virtual BGF to the Gateway Controller

For seamless interoperability between the BGF and gateway controller devices, you can control the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller. You can also prevent the system from being overloaded with messages for certain state changes by specifying that the virtual BGF not send a request or notification when those changes occur.

You can specify the method and reason that the virtual BGF includes in ServiceChange commands when the state of one of the following changes:

- Control associations
- Virtual interfaces
- Contexts

Control Association States

A control association is a relationship where the gateway controller is controlling the virtual BGF. Each virtual BGF has only one control association at any time.

Table 6 on page 126 describes the control association states.

Table 6: Control Association States

Control Association State	Description
Disconnected	The control association is in the Disconnected state. No gateway controller is controlling the virtual BGF, and incoming H.248 messages are ignored. The control association remains disconnected as long as the virtual BGF is Out-of-Service. Depending on what caused the virtual BGF to become Out-of-Service, the virtual BGF either drops H.248 commands or answers them with a port-unreachable ICMP error.
Connecting	The control association is in Connecting state between the time the virtual BGF sends a registration request to the gateway controller and the time the gateway controller accepts, rejects, or aborts the request. The virtual BGF rejects incoming H.248 commands while the control association is in the Connecting state with error # 505: "Transaction Request Received before a ServiceChange Reply has been received".
Draining	The control association enters the Draining state when an administrator instructs the virtual BGF to gracefully transition from In-Service to Out-of-Service. The gateway controller transitions to Out-of-Service when the controlling gateway controller subtracts all of the virtual BGF's H.248 terminations. The virtual BGF accepts only Subtract and AuditValue commands from the controlling gateway controller. It rejects all other commands with error # 502: "Not Ready".

When the state of a control association changes, the virtual BGF can send the following types of ServiceChange commands to the gateway controller:

- Registration Requests—The virtual BGF sends a Registration Request ServiceChange command to request that a gateway controller become its controlling gateway controller. The virtual BGF sends these requests when a control association enters the Connecting state.
- Unregistration Messages—The virtual BGF sends an Unregistration ServiceChange command to its controlling gateway controller when it transitions to the Out-of-Service (Disconnected) service state because of an administration operation or a failure. The failure can be the result of a services PIC, Flexible PIC Concentrator (FPC), or MS-DPC failure, or because the PIC or DPC was powered off or removed.
- Notification Messages—The virtual BGF sends a notification ServiceChange command to its controlling gateway controller when the control association transitions between the Connected and Draining states and vice versa.

Method and Reason Options for Control Association State Changes

You can control the ServiceStateMethod and ServiceStateReason that the virtual BGF includes in ServiceChange commands for control associations.

You can use the CLI to specify the method and reason that the virtual BGF includes in ServiceChange commands for control associations. Table 7 on page 127 shows the method and reason options available for each reported state and the events that led to the report.

Table 7: Options for Method and Reason in ServiceChange Commands for Control Associations

Reported Association State	Event Leading to Report	Options	Embedded H.248 Reason	Explanation
Disconnect	Controller failure	FL/909	Gateway controller impending failure	Virtual BGF is reregistering with a new gateway controller following a disconnection of the virtual BGF and gateway controller.
		RS/902	Warm boot	Virtual BGF is reregistering with a new gateway controller following a disconnection of the virtual BGF and gateway controller.
	Reconnect	DC/900	Service restored	Virtual BGF is registering with the last controlling gateway controller following a disconnection of the virtual BGF and gateway controller.
		RS/902	Warm boot	Virtual BGF is transitioning to In-Service, and the previously installed state is retained.
Down	Administrative	FO/905	Termination taken out of service	Virtual BGF is transitioning to Out-of-Service because of an administrative operation.
		FO/908	VPG impending failure	Virtual BGF root termination transitioned to Out-of-Service and is unable to process request.
		none		No message is sent for this event.
	Failure	FO/904	Termination malfunctioning	Virtual BGF is transitioning to Out-of-Service because of a failure.
		FO/908	VPG impending failure	Virtual BGF root termination transitioned to Out-of-Service because of a failure.
		none		No message is sent for this event.
	Graceful	GR/905	Termination taken out of service	The control association entered the Draining state because of an administrative operation.
		none		No message is sent for this event.

Table 7: Options for Method and Reason in ServiceChange Commands for Control Associations *(continued)*

Reported Association State	Event Leading to Report	Options	Embedded H.248 Reason	Explanation
Up	Cancel graceful	RS/908	Cancel graceful	The control association transitioned from the Draining state to the Forwarding state.
		none		No message is sent for this event.
	Cold failover	FL/920	Cold failover	Virtual BGF is registering following a graceful Routing Engine switchover. The previously installed state is reset.
		RS/901	Cold boot	Virtual BGF is transitioning to In-Service. The previously installed state is not retained.
	Warm failover	FL/919	Gateway controller impending failure	Virtual BGF is registering with a new gateway controller following a disconnection of the virtual BGF and gateway controller.
		RS/902	Warm boot	Virtual BGF is transitioning to In-Service, and the previously installed state is retained.

Configuring the Method and Reason in ServiceChange Commands for Control Associations

Step-by-Step Procedure

To configure the method and reason in ServiceChange commands for control associations:

1. Access the configuration of the service change control association indications properties.

```
[edit services pgcp]
user@host#edit gateway bgf-1 h248-options service-change
   control-association-indications
```

2. Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.

```
[edit services pgcp gateway bgf-1 h248-options service-change
   control-association-indications]
user@host#set disconnect controller-failure restart-902
```

3. Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set disconnect reconnect restart-902
```

4. Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set down administrative forced-908
```

5. Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of a failure.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set down failure forced-904
```

6. Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set down graceful graceful-905
```

7. Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association has returned to the Connected state.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set up cancel-graceful restart-918
```

8. Specify the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a cold failover.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set up failover-cold failover-920
```

9. Specify the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a warm failover.

```
[edit services pgcp gateway bgf-1 h248-options service-change
  control-association-indications]
user@host#set up failover-warm restart-902
```

Virtual Interface States

Table 8 on page 130 describes the virtual interface states.

Table 8: Virtual Interface States

Virtual Interface Operational State	Description
Blocked	A virtual interface is in the Blocked state when the interface is Out-of-Service. While a virtual interface is in the Blocked state, all VPGs do not add new terminations using the interface. Likewise, the virtual BGF rejects H.248 commands other than Subtract and AuditValue commands on existing terminations on the interface. The error that the virtual BGF returns for commands that it rejects depends on the reason that caused the virtual interface to be Out-of-Service: ■ Error #502: "Not ready"—If the virtual interface is Out-of-Service because of an administrative operation. ■ Error #529: "Internal hardware failure in PG"—If the virtual interface is Out-of-Service because of a failure.
Forwarding	A virtual interface is in the Forwarding state when it is functioning normally. All gates are using the interface process data flows according to the H.248 properties installed on them.
Draining	A virtual interface enters the Draining state when an administrator instructs the virtual interface to gracefully transition from In-Service to Out-of-Service. The virtual interface automatically transitions to Out-of-Service when it is no longer used by any termination in any of the virtual BGFs. A virtual interface that is in the Draining state is In-Service and existing gates process data flows normally. However, as in the Blocked state, the virtual BGFs do not add new terminations using that virtual interface or to perform any command other than Subtract and AuditValue on existing terminations on the interface. If the virtual BGF receives other commands, it replies with error #502: "Not ready".

When the state of a virtual interface changes, the virtual BGF can send the following types of ServiceChange commands to the gateway controller:

- Service-Restoration—The virtual BGF sends Service-Restoration ServiceChange commands when a virtual interface transitions to the In-Service service state; that is, it transitions from the Blocked state to the Forwarding operational state.
- Service-Interruption—The virtual BGF sends Service-Interruption ServiceChange commands when a virtual interface transitions to the Out-of-Service, or Blocked, service state.
- Notification Messages—The virtual BGF sends Notification ServiceChange commands when a virtual interface transitions between the Forwarding and Draining states and vice versa.

Method and Reason Options for Virtual Interface State Changes

You can control the ServiceStateMethod and ServiceStateReason that the virtual BGF includes in ServiceChange commands for virtual interface state changes.

You can use the CLI to specify the method and reason that the virtual BGF includes in ServiceChange commands for virtual interfaces. Table 9 on page 131 explains the method and reason options available for each reported state and the events that led to the report.

Table 9: Options for Method and Reason in ServiceChange Commands for Virtual Interfaces

Reported State	Event Leading to Report	Options	Embedded H.248 Reason	Explanation
Virtual interface down	Administrative	FO/905	Termination taken out of service	Virtual interface is transitioning to Out-of-Service because of an administrative operation.
		FO/906	Loss of lower-layer connectivity	Virtual interface is transitioning to Out-of-Service because of a loss of layer 2 connectivity caused by the logical or physical interface being administratively disabled.
		none		No message is sent for this event.
	Graceful	GR/905	Termination taken out of service	Virtual interface has entered the Draining state.
		none		No message is sent for this event.
Virtual interface up	Cancel graceful	RS/918	Cancel graceful	Virtual interface has returned to the Forwarding state.
		none		No message is sent for this event.
	warm	RS/900	Service restored	Virtual interface has become In-Service and is in the Forwarding state.
		none		No message is sent for this event.

Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces

Step-by-Step Procedure

To configure the method and reason in ServiceChange commands for virtual interfaces:

1. Access the configuration of the service change virtual interface indications properties.

```
[edit services pgcp]
user@host#edit gateway bgf-1 h248-options service-change
   virtual-interface-indications
```

2. Specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when a virtual interface changes to Out-of-Service because of an administrative operation.

   ```
   [edit services pgcp gateway bgf-1 h248-options service-change
     virtual-interface-indications]
   user@host#set virtual-interface-down administrative forced-906
   ```

3. Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when a virtual interface transitions between the Forwarding and Draining states.

   ```
   [edit services pgcp gateway bgf-1 h248-options service-change
     virtual-interface-indications]
   user@host#set virtual-interface-down graceful none
   ```

4. Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the virtual interface transitions from the Draining state to the Forwarding state.

   ```
   [edit services pgcp gateway bgf-1 h248-options service-change
     virtual-interface-indications]
   user@host#set virtual-interface-up cancel-graceful restart-918
   ```

5. Specify the method and reason that the virtual BGF includes in Service-Restoration ServiceChange commands that it sends to the gateway controller when a virtual interface transitions to In-Service.

   ```
   [edit services pgcp gateway bgf-1 h248-options service-change
     virtual-interface-indications]
   user@host#set virtual-interface-up warm restart-900
   ```

Context States

The virtual BGF sends context Service-Interruption messages when the gates of a specific context no longer provide their configured service. When such a message is issued, both terminations included in the context become Out-of-Service.

You can use the CLI to specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when a state loss occurs. Table 10 on page 133 describes the method and reason options available.

Table 10: Options for Method and Reason in ServiceChange Commands for Specific Contexts

Reported State	Event Leading to Report	Options	Embedded H.248 Reason	Explanation
State loss	Mismatch between pgcpd process and Service PIC or MS-DPC states	FO/910	State loss because of a media failure	A mismatch between the pgcpd process and the services PIC or MS-DPC states was detected on one or more of the context's gates.
		FO/915	State loss	A mismatch between the pgcpd process and the services PIC or MS-DPC states was detected on one or more of the context's gates.
		none		No message is sent for this event.

Configuring the Method and Reason in ServiceChange Commands for Contexts

Step-by-Step Procedure

To configure the method and reason in ServiceChange commands for contexts:

1. Access the configuration of the service change context indications properties.

```
[edit services pgcp]
user@host#edit gateway bgf-1 h248-options service-change context-indications
```

2. Specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller after a state loss on a specific context.

```
[edit services pgcp gateway bgf-1 h248-options service-change context-indications]
user@host#set state-loss forced-915
```

Chapter 7

Upgrade Guidelines for BGF VoIP Users

Upgrade Overview for BGF VoIP Users

As a voice user, exercise caution in preparing for and executing a software upgrade. By doing so, you can ensure the proper handling of emergency calls and minimize overall disruption of service to customers. The following list describes how to prepare to upgrade a router used for voice processing.

- Back up—Back up your current configuration.
- Upload new software—In a dual RE configuration, upload the software to the backup RE.
- Redirect—Configure gateway controllers to redirect calls for all virtual BGFs on the device to virtual BGFs not subject to the upgrade. Refer to the documentation for your gateway controller for details.
- Perform a graceful shutdown of all virtual BGFs—Initiate a graceful shutdown for each virtual BGF to prevent initiation of new calls.

  For detailed information on how to perform a graceful shutdown, refer to "Shutting Down a Virtual BGF" on page 116.
- Check emergency calls—For each virtual BGF, confirm that no emergency calls are active.

  For detailed information on checking active calls, refer to "Managing Emergency and Non-Emergency Call Traffic Prior to Upgrading" on page 136.
- Check remaining active calls—For each virtual BGF, continue checking active calls until either none remain or you force the shutdown of the virtual BGF to terminate remaining non-emergency calls.
- Upgrade—Refer to the *JUNOS Software Installation and Upgrade Guide* for detailed upgrade instructions.

Managing Emergency and Non-Emergency Call Traffic Prior to Upgrading

Before you upgrade a router that you are using for voice traffic, monitor call traffic on each virtual BGF. Confirm that no emergency calls are active. When you have determined that no emergency calls are active, you can wait for non-emergency call traffic to drain due to the graceful shutdown, or you can force a shutdown.

To check the status of emergency and non-emergency calls

1. Log in to the router.
2. Enter the following operational mode command to display the total number of active contexts and the number of active emergency contexts:

```
user@host> show services pgcp statistics gateway bgf-1 extensive match |
contexts

Contexts : 11 / 6000

Emergency contexts        :  0
```

3. Repeat 2 until the number of emergency contexts is 0.
4. As a precaution, also query the gateway controller to confirm there are no active emergency calls. Refer to the documentation for your gateway controller for details.
5. Repeat 2 until no contexts are active or you decide to force a shutdown of the virtual BGF.

Chapter 8

Maintenance and Failover in the BGF

This chapter describes maintenance and failover processes for the BGF. Topics include:

Maintenance and Failover in the BGF Overview

By providing redundancy for both the Routing Engine and the service PICs, the BGF high-availability (HA) architecture allows for a multilevel redundant solution. This solution ensures service and call continuity, which is necessity for VoIP services.

Figure 24 on page 137 shows the BGF HA architecture.

Figure 24: BGF HA Architecture

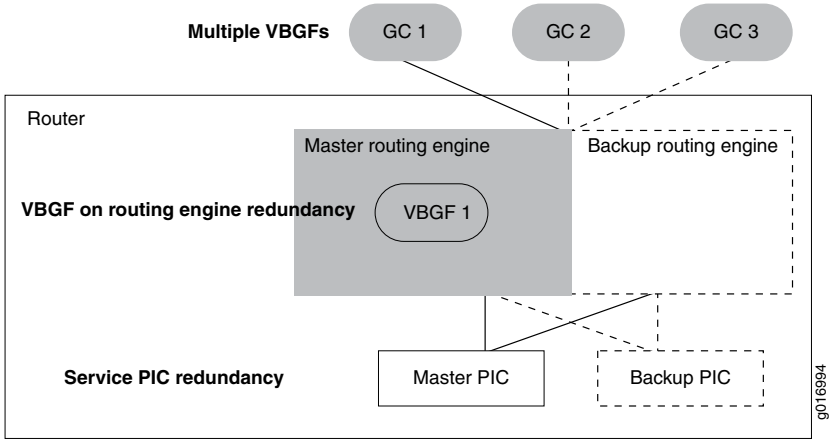


Table 11 on page 138 indicates how service PIC or MS-DPC failure and Routing Engine failure affect different types of services.

Table 11: How Service PIC and Router Engine Failures Affect Service and Call Continuity

Service	Service PIC or MS-DPC Failure	Routing Engine Failure
Stable H.248 contexts	Call continuity—All calls are lost. Service continuity—Provided when the backup PIC or DPC is available.	Call continuity—All existing calls are maintained through the failure Service continuity—New calls and session can be established when the backup Routing Engine takes control.
H.248 contexts are modified	Call continuity—All existing call states are lost. Service continuity—Calls and sessions that are in a Setup state (gates and terminations not fully defined) are lost	Call continuity—All existing call states are lost. Service continuity—Calls and sessions that are in a Setup state are lost.
Connection to the gateway controller	Call continuity—All calls are lost. Service continuity—Provided when the backup service PIC or DPC is available.	Call continuity—No calls are lost. Service continuity—Provided when the backup Routing Engine takes control.

Failover in Case of a Routing Engine Failure

Graceful Routing Engine switchover (GRES) is supported in case of a Routing Engine failure. A failure of the Routing Engine stops the pgcpd process. When the JUNOS Software high-availability framework detects the Routing Engine failure, it switches control of the BGF to the pgcpd process on the backup Routing Engine. The pgcpd process stores completed H.248 states, and these states survive a restart or a switchover. After the restart or switchover is completed, the pgcpd process reapplies the states.

Gate Synchronization Procedure

When the IPC connection between the pgcpd process and the services PIC or MS-DPC is being reestablished, a synchronization process restores the previous state of gates, so session and call continuity is achieved. That is, existing calls stay active and voice sessions are not disconnected.

The synchronization process can result in the mismatching of gates. Mismatched gates are handled as follows:

- If the pgcpd process detects gates that exist in the Routing Engine, but are missing in the PIC or DPC, the pgcpd process reinstalls the gates on the PIC or DPC. Existing calls receive service from the PIC or DPC when the synchronization is complete.
- If the pgcpd process detects gates that exist on the PIC or DPC, but not on the Routing Engine, the pgcpd process removes the gates from the PIC or DPC. This removal causes the associated sessions to be closed, and the session resources to be released.
- If the pgcpd process detects gates that exist on the PIC or DPC and on the Routing Engine, but the versions of the gates do not match, the pgcpd process forces the Routing Engine version. Doing so maintains call continuity by making sure that

the databases are synchronized, while limiting the effect to existing calls and sessions.

You can control the number of mismatches by configuring the synchronization properties.

Configuring Synchronization Properties

You can configure the maximum number of mismatches allowed during the synchronization process between the PIC or DPC and the pgcpd process.

Step-by-Step Procedure To configure properties for synchronization between the PIC or DPC and the pgcpd process:

1. Access the graceful restart configuration.

   ```
   [edit services pgcp]
   edit gateway bgf-1 graceful-restart
   ```

2. Configure the maximum number of mismatches allowed during the synchronization procedure. If the number of mismatches exceeds this number, the pgcpd process clears the state of the PIC or DPC and the state of the pgcpd process. All calls and sessions are terminated and existing resources are released.

   ```
   [edit services pgcp gateway bgf-1 graceful-restart]
   user@host#set maximum-synchronization-mismatches 20
   ```

3. Configure the number of milliseconds within which you want the synchronization process to complete. If the process is not complete when this time expires, the pgcpd process clears the state of the PIC or DPC and the state of the pgcpd process.

   ```
   [edit services pgcp gateway bgf-1 graceful-restart]
   user@host#set maximum-synchronization-time 300
   ```

Displaying the Status of the Routing Engine Synchronization

Purpose To determine the status of the synchronization between the main Routing Engine and the backup Routing Engine, display the value of the replication socket field.

Action

```
user@host> show services pgcp active-configuration
. . .
Virtual BGF configuration:
  Name                                  :  bgf-1
  IP address                            :  10.10.10.1
  Port                                  :  2944
  Status                                :  In-Service (Registered)
  Active gateway controller             :  dt3
  Cleanup timeout [secs]                :  3600
  Gate inactivity delay [secs]          :  240
  Gate inactivity duration (Q-MI ) [secs]  :  86400
  Replication socket                    :  Disconnected

. . .
```

Meaning The replication socket can be in one of the following states:

- Connected (Ready)—The replication is ready, and it is safe to perform a switchover.
- Connected (Syncing)—The replication is synchronizing. It is not safe to perform a switchover.
- Connected (Error)—An error occurred in the previous switchover.
- Disconnected—The backup Routing Engine is down. It is not safe to perform a switchover because there is no backup Routing Engine.

Related Topics

- *Part 3, Graceful Routing Engine Switchover* in *JUNOS High Availability Configuration Guide*
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Failover of the Data Service PICs

The data PIC failover procedure for the BGF assures service continuity in case of a service PIC failure. The BGF architecture provides both a 1:1 redundancy model and a 1:N redundancy model for data service PICs.

In the 1:1 redundancy model, there is one primary service PIC and one secondary service PIC that acts as a backup. If the primary service PIC fails, the Routing Engine allocates the secondary service PIC, and the software switches over to the secondary service PIC. The pgcpd process continues to provide the PGCP services as if the service PIC has restarted. All states and sessions are lost, but new calls are accepted. When the failed service PIC recovers, it does not take over from the redundant PIC.

In the 1:N redundancy model, you can define one PIC as the secondary of many primary PICs. In this model, after the secondary PIC becomes active, all other primary PICs are left without a secondary PIC. Even when the primary PIC recovers, it does not become a redundant PIC to all of the primary PICs. A recovered primary PIC can replace only the same secondary PIC that previously replaced it. This functionality means that administrative involvement is usually required after a failover event happens.

Procedure in Case of Data PIC Failure

If a data PIC fails, the following procedure takes place:

1. Active calls are lost.
2. The BGF notifies the gateway controller of the failure using an FO/904 ServiceChange message.
3. The BGF receives an acknowledgment for the FO/904 message from the gateway controller.

4. The redundant service PIC (rsp) mechanism allocates the secondary PIC and makes the secondary PIC the new primary PIC.
5. The new primary PIC establishes the IPC connection to the pgcpd process on the routing engine.
6. The pgcpd process issues an RS/902 registration message to the gateway controller.
7. The pgcpd process receives an acknowledgment of the registration message from the gateway controller.
8. The BGF is ready to accept and process new H.248 commands.

Configuring the BGF for Data PIC Redundancy

To configure data PIC failover, you configure a redundancy services PIC (rsp) interface that specifies which service PIC is the primary PIC and which service PIC is the secondary PIC. In the service set configuration for the PGCP service, the service set points to the rsp interface as the next-hop service interface.

You can configure a redundant pair of service PICs to operate in *hot standby* mode, facilitating faster switching to the standby PIC in a failover situation. Changes are applied to both of the paired PICs simultaneously. This differs from the default, *warm standby*, in which the standby PIC receives configuration information at the time of failover. The maximum switchover time for *hot standby* is 5 seconds. A typical failover time depends on the failure conditions and can be much less than the maximum.

Configuring the Redundancy Services PIC (rsp) Interface

To configure, create a redundancy services PIC (rsp) interface, and specify the primary and secondary service PIC and the inside and outside service domains.

Step-by-Step Procedure To configure the rsp interface:

1. Configure the interface, and enter edit mode for the interface.

```
[edit]
user@host#edit interfaces rsp1
```

2. Specify the service PIC that is to be the primary PIC.

```
[edit interfaces rsp1]
user@host#set redundancy-options primary sp-1/2/0
```

3. Specify the service PIC that is to be the secondary PIC.

```
[edit interfaces rsp1]
user@host#set redundancy-options secondary sp-1/3/0
```

4. (Optional) Configure hot standby to ensure that failover occurs in 5 seconds or less.

```
[edit interfaces rsp1]
user@host#set redundancy-options hot-standby
```

5. Configure a logical unit and specify the protocol family.

```
[edit interfaces rsp1]
user@host#set unit 10 family inet
```

6. Set the service domain of the logical unit to inside. This unit number must match the unit number of the inside service interface configured in the service set.

```
[edit interfaces rsp1]
user@host#set unit 10 service-domain inside
```

7. Configure another logical unit and specify the protocol family.

```
[edit interfaces rsp1]
user@host#set unit 20 family inet
```

8. Set the service domain of the logical unit to outside. This unit number must match the unit number of the outside service interface configured in the service set.

```
[edit interfaces rsp1]
user@host#set unit 20 service-domain outside
```

Configuring the Service Set for Redundant Service PICS

When you configure your service set, specify the rsp interface as the next-hop service.

Step-by-Step Procedure To configure a service set for redundancy:

1. Create a service set configuration.

```
[edit services]
user@host#edit service-set bgf-svc-set
```

2. Configure service set as a next-hop service set.

```
[edit services service-set bgf-svc-set]
user@host#edit next-hop-service
```

3. Specify the rsp interface to the inside network. This unit number must match the unit number of the inside service domain configured in the rsp interface.

```
[edit services service-set bgf-svc-set next-hop-service]
user@host#set inside-service-interface rsp1.10
```

4. Specify the rsp interface to the outside network. This unit number must match the unit number of the outside service domain configured in the rsp interface.

```
[edit services service-set bgf-svc-set next-hop-service]
user@host#set outside-service-interface rsp1.20
```

Manually Switching from the Primary PIC to the Secondary PIC

Purpose Manually switch from the primary PIC to the secondary PIC.

Action

```
user@host>  request interface rsp1 switchover
request succeeded
```

Manually Reverting from the Secondary PIC to the Primary PIC

Purpose Manually revert from the secondary PIC to the primary PIC.

Action

```
user@host> request interface rsp1 revert
request succeeded
```

Displaying the Status of the Redundant Service PICs

Purpose Display the status of the redundant service PICs. You can use this command to determine which PIC is currently active.

Action

```
user@host> show interface redundancy rsp1
Interface  State            Last change  Primary    Secondary  Current status
rsp1       On primary     00:25:18        sp-1/2/0    sp-1/3/0        both up
```

Related Topics

- *Chapter 24, Interface Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 19, Adaptive Services Interface Operational Mode Commands* in *JUNOS Interfaces Command Reference*

Failover of the Control Service PICs

If you are running the pgcpd process on services PICs, you can use a 1:1 redundancy model to pair two services PICs in high availability mode using a virtual redundant MultiServices PIC (rms) interface. As part of the configuration, one of the PICs is set as the primary and the other as the secondary PIC. When the rms interface comes up, the primary PIC comes up as active and the secondary PIC as standby.

On failure of the active PIC, the standby PIC becomes active and traffic is switched over to the new active PIC. When the failed primary PIC is restored, it comes up as standby. You must explicitly request a reversion to the primary PIC to make it active again. Otherwise, it continues in standby mode until the active PIC fails.

Configuring the rms Interface

To configure, create an rms interface and specify the primary and secondary service PIC and the inside and outside service domains. When a new rms interface is created, PICs designated as primary and secondary reboot automatically. If either the primary or secondary PIC, or both, are changed, the corresponding old and new ms- interfaces reboot automatically.

Step-by-Step Procedure To configure the rms interface:

1. Configure the interface, and enter edit mode for the interface.

   [edit]

```
user@host#edit interfaces rms0
```

2. Specify the service PIC that is to be the primary PIC.

```
[edit interfaces rms0]
user@host#set redundancy-options primary ms-1/2/0
```

3. Specify the service PIC that is to be the secondary PIC.

```
[edit interfaces rms0]
user@host#set redundancy-options secondary ms-1/3/0
```

4. (Optional) Configure hot standby to ensure that failover occurs in 5 seconds or less.

```
[edit interfaces rms0]
user@host#set redundancy-options hot-standby
```

5. Configure a logical unit and specify the protocol family.

```
[edit interfaces rms0]
user@host#set unit 0 family inet
```

Specify the rms Interface as the Platform Device for the Virtual BGF

In your virtual BGF configuration, configure the rms interface as the platform device for the virtual BGF. For example:

```
[edit services pgcp gateway bgf-1]
user@host#set platform device rms0
```

Manually Switching from the Primary PIC to the Secondary PIC

Purpose Manually switch from the primary PIC to the secondary PIC. After the switchover, we recommend that you place the old active PIC offline temporarily so it comes up fresh as a new backup.

Action

```
user@host> request interface rms0 switchover
request succeeded
```

Manually Reverting from the Secondary PIC to the Primary PIC

Purpose Manually revert from the secondary PIC to the primary PIC.

Action

```
user@host> request interface rms0 revert
request succeeded
```

Displaying the Status of the Redundant Service PICs

Purpose Display the status of the redundant service PICs. You can use this command to determine which PIC is currently active.

Action

```
user@host> show interface redundancy rms1
Interface   State           Last change    Primary   Secondary  Current status
rms0         Not present                   ms-1/2/0  ms-1/3/0     both up
rms1         On secondary   1d 23:56       ms-1/1/0  ms-0/2/0     primary down
rms2         On primary     10:10:27       ms-1/3/0  ms-0/2/0     secondary down
```

Chapter 9

Troubleshooting the BGF

This chapter explains how to set up trace options for the BGF and the logging of H.248 messages. Topics include:

Tracing BGF Operations

You can trace the following BGF components and record trace results in a log file:

- BGF core
- H.248 stack
- SBC utilities

All log files are placed in the /var/log directory. When a trace file reaches its maximum size, a .0 is appended to the file name, then a new file is created with a .1 appended, and so on. When the maximum number of trace files is reached, the oldest trace file is overwritten.

Step-by-Step Procedure To configure tracing of BGF operations:

1. Access the traceoptions file configuration.

   ```
   [edit]
   user@host# edit services pgcp traceoptions file
   ```

2. Specify a name for the trace file.

   ```
   [edit services pgcp traceoptions file]
   user@host# set filename bgf1
   ```

3. Set the maximum number of trace files. If you specify a maximum number of files, you also must specify a maximum file size.

   ```
   [edit services pgcp traceoptions file]
   user@host# set files 10
   ```

4. Set user access to the trace log file. Use set no-world-readable to prevent users from accessing the log file, or use set world-reabable to all any user to read the log file.

```
[edit services pgcp traceoptions file]
user@host# set no-world-readable
```

5. Access the traceoptions flag configuration to define trace level options.

```
[edit services pgcp traceoptions file]
user@host# up
[edit services pgcp traceoptions]
user@host# edit flag
```

6. Specify the operations that you want to include in the log file. For example:

```
[edit services pgcp traceoptions flag]
user@host# set bgf-core firewall warning
user@host# set bgf-core pic-broker warning
user@host# set h248-stack control-association warning
user@host# set sbc-utils memory-management debug
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Tracing BGF Operations for a Specific Control Services PIC

If you are running the pgcpd process on services PICs, you can trace log messages separately for each services PIC on which the pgcpd process is running. To do so, you need to send messages to the var/log/messages file. The operations that you specify at the [edit services pgcp traceoptions flag] hierarchy are included in the messages log file.

Step-by-Step Procedure

To configure logging of messages for a services PIC:

1. Access the system syslog configuration.

```
[edit]
user@host# edit system syslog
[edit system syslog]
```

2. Specify that traces are logged to the messages file. Include the severity level that you want to log. In this example, the severity level is any.

```
[edit system syslog]
user@host# set file messages daemon any
```

3. Enable PIC system logging to record system log messages on a specific PIC. The following example sets up logging on the FPC in slot 1 and the PIC in slot 0.

```
user@host# set chassis fpc 1 pic 0 adaptive-services service-package
  extension-provider syslog daemon any
```

Logging Messages for the pgcpd Process Running on the Routing Engine

The pgcpd process produces syslog messages for many of its functions. You can configure selection criteria for saving pgcpd messages in a log trace file.

All log trace files are placed in the /var/log directory. When a trace file reaches its maximum size, a .0 is appended to the file name, then a new file is created with a .1 appended, and so on. When the maximum number of trace files is reached, the oldest trace file is overwritten.

Step-by-Step Procedure To configure logging of pgcpd syslog messages:

1. Access the system syslog configuration.

```
[edit]
user@host# edit system syslog
[edit system syslog]
```

2. Configure the file parameters. In the example, the file is named myfile and all messages with a severity equal to or greater than error.

```
[edit system syslog]
user@host# set file myfile error
```

3. Configure the match parameter to select pgcpd syslog messages.

```
[edit system syslog]
user@host# set match pgcpd
```

4. (Optional) To direct output to one or more user consoles, configure the user parameter.

```
user@host# set user testuser
```

Related Topics For more information on the options available when configuring system log messages, refer to:

- *Chapter 1, Configuring System Log Messages* in the *JUNOS System Log Messages Reference*.

Logging H.248 Messages

You can use the traceoptions feature to log H.248 messages exchanged between a virtual BGF and its associated gateway controller. These messages can include all transactions, transaction replies, and transaction acknowledgements, depending on the specified trace level. Corrupted messages, messages with invalid syntax, and messages that fail interim AH validation can also be logged. The captured data includes both the raw H.248 message (as it appears on the wire) and associated metadata.

The captured data is stored by default in the pgcpd file in the /var/log directory. In addition to H.248 messages, this file contains all other BGF operations that you have

chosen to trace. To make it easier to find H.248 messages in the file, there is a BEGIN field and an END field, each with a matching sequence number.

When you enable logging of H.248 messages, the software logs messages for all virtual BGFs on the router. To determine which virtual BGF exchanged the message, use the 5-tuple field in the H.248 message.

Fields in the H.248 Messages

Each H.248 message contains the following fields:

```
TRACE_TIMESTAMP
[BEGIN #SEQNUM  TIMESTAMP  5-TUPLE  DIRECTION  MSG_SIZE]
MegacoMessage
[END #SEQNUM]
```

The following is a sample ServiceChange message:

```
Oct 10 09:32:28
[BEGIN #778  Oct 10 09:32:28  UDP:10.50.40.100:2944->172.16.1.1:2944  TX  168]
AU=0x00000000:0x00000000:0x00000000000000000000000000
!/1 [10.50.40.100]:2944
T=1{
C=-{
SC=ROOT{
SV{MT=RS,RE="901",AD=2944,PF=JNPR_PGCP/1,V=3,20071010T09322800}}}}
[END #778]
```

Table 12 on page 150 describes the fields in H.248 messages.

Table 12: Description of Fields in H.248 Messages

Field	Description
TRACE_TIMESTAMP	Time the messaged was captured. The timestamp is in the format *HH:MM:SS.mmmmmm*
BEGIN	Constant string BEGIN that indicates the beginning of a message.
#SEQNUM	Sequential number of the message used to correlate the BEGIN header with the END footer.
TIMESTAMP	Date and time of the message. Time is displayed in the format *HH:MM:SS.mmmmmm*
5-TUPLE	UDP or TCP packet's 5-tuple (transport protocol, source address and port, destination address and port). Used to identify the virtual BGF and the gateway controller that exchanged the message.
DIRECTION	Direction message was sent from the virtual BGF: ■ TX for an outgoing H.248 message. ■ RX for an incoming H.248 message.
MSG_SIZE	Size of message in bytes excluding transport protocol (UDP/TCP/IP) overhead.
MegacoMessage	Captured data including the interim authentication header (if any).
END	Constant string END that indicates the end of a captured message.

Messages That Exceed Output Buffer Limit

The trace file has a limit on the size of a single output buffer. Messages longer than this limit are divided into several trace buffers. Messages divided into buffers use the following template:

```
TRACE_TIMESTAMP
  [BEGIN #SEQNUM  TIMESTAMP  5-TUPLE  DIRECTION  MSG_SIZE]
  MegacoMessage (1st part)
  TRACE_TIMESTAMP (--- contd ---)
  MegacoMessage (2nd part)
  ...
  TRACE_TIMESTAMP (--- contd ---)
  MegacoMessage (n'th part)
  [END #SEQNUM]
```

Here is an example of a divided message:

```
Oct 10 09:32:56
  [BEGIN #779  Oct 10 09:32:56  UDP:22.0.0.6:2944->10.50.40.100:2944  RX  436]
  AU=0x00000000:0x00000000:0x00000000000000000000000000
  MEGACO/3 [22.0.0.6]:2944
  Transaction = 12567418{
      Context = 65323 {
         Modify=ip/4/vif-0/3 {
            Media{
               Stream=1{
                  LocalControl{Mode=SR,DS/DSCP=00,TMAN/POL=on}}}},
         Modify=ip/4/vif-0/3 {
            Media{
               Stream=1{
  Oct 10 14:13:19 (--- contd ---)
                  LocalControl{Mode=SR,DS/DSCP=00,TMAN/POL=on}}}}}}
  [END #779]
```

Configuring Logging of H.248 Messages

The captured data is stored by default in the pgcpd file in the /var/log directory.

Step-by-Step Procedure To enable logging of H.248 messages:

1. Access the PGCP traceoptions configuration.

   ```
   [edit]
   user@host#edit services pgcp traceoptions
   ```

2. Set the flag that enables logging of H.248 messages.

   ```
   [edit services pgcp traceoptions]
   user@host#set flag h248-stack messages
   ```

3. Set the maximum number of trace files.

   ```
   [edit services pgcp traceoptions]
   user@host#set file files 10
   ```

4. Set the maximum size of the trace files.

```
[edit services pgcp traceoptions]
user@host#set file size 10000k
```

5. Set the availability of the trace files to all users.

```
[edit services pgcp traceoptions]
user@host#set file world-readable
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Chapter 10

Example: Using the BGF to Provide VoIP Solutions in a Next-Generation Network

This example describes how to configure the BGF VoIP solution on a router in the service provider core network. Topics include:

Requirements

This example uses the following software and hardware components:

- JUNOS Release 9.0 or later
- Juniper Networks T640 Core Router with a MultiServices 500 PIC

Overview and Topology

This example shows how to configure the SP BGF router in the topology shown in Figure 25 on page 154.

Figure 25: Voice Solution Topology Diagram

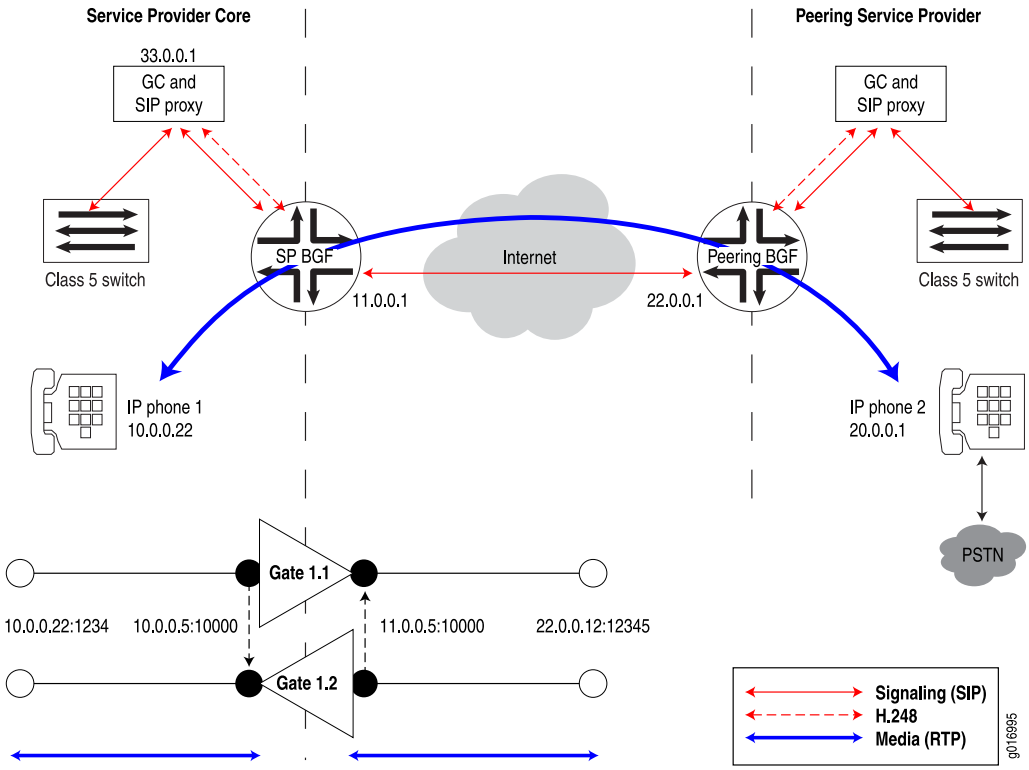


Table 13 on page 155 shows the voice configuration components.

Table 13: Addresses Used in the Voice Solution Topology

Device	Interfaces/Virtual BGF/NAT Pools	Address
SP BGF (Service Provider BGF)	sp–1/2/0.10 (inside service domain for BGF-1)	Not applicable
	sp-1/2/0.20 (outside service domain for BGF-1)	
	sp-1/2/0.30 (inside service domain for BGF-2)	
	sp-1/2/0.40 (outside service domain for BGF-2)	
	sp-1/2/1.10 (inside service domain for BGF-3)	Not applicable
	sp-1/2/1.20 (outside service domain for BGF 3)	
	BGF-1—Provides both SIP and RTP over IPv4	172.16.10.1
	BGF-2—Provides RTP (video) over IPv4	172.16.20.2
	BGF-3—Provides media over IPv6	172.16.30.3
	Media (RTP) NAT Pools	Pool Address
	■ bgf1_peer_rtp-nat-pool-1	■ 11.0.0.5
	■ bgf2_peer_rtp-nat-pool-2	■ 11.0.0.25
	■ bgf3_peer_rtp-nat-pool-3	■ 2001:db8:10:3::100/128
	■ bgf1_core_rtp-nat-pool-4	■ 10.0.0.5
	■ bgf2_core_rtp-nat-pool-5	■ 10.0.0.25
	■ bgf3_core_rtp-nat-pool-6	■ 2001:db8:13:2::100/128
	Signaling (SIP) NAT Pools	Pool Address
	■ bgf1_peer_sip-nat-pool-7	■ 11.0.0.2
	■ bgf1_core_sip-nat-pool-8	■ 10.0.0.2
Gateway Controller		33.0.0.1
Peering Router		22.0.0.1

Configuration

To configure the SP BGF router:

- Configuring the Service Interfaces on page 158
- Configuring the Virtual BGFs on page 160
- Configuring NAT Pools on page 162
- Assigning the NAT Pools to a Media Service on page 166
- Configuring the Virtual Interfaces on page 167
- Configuring Rules for the BGF on page 168
- Configuring a Stateful Firewall on page 170

- Configuring a Service Set on page 170
- Configuring QoS for Voice Calls on page 172

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

```
[edit]
set interfaces sp-1/2/0 description bgf1_bgf2_pgcp_service_ipv4
set interfaces sp-1/2/0 unit 0 family inet
set interfaces sp-1/2/0 unit 10 family inet
set interfaces sp-1/2/0 unit 10 service-domain inside
set interfaces sp-1/2/0 unit 20 family inet
set interfaces sp-1/2/0 unit 20 service-domain outside
set interfaces sp-1/2/0 unit 30 family inet
set interfaces sp-1/2/0 unit 30 service-domain inside
set interfaces sp-1/2/0 unit 40 family inet
set interfaces sp-1/2/0 unit 40 service-domain outside
set interfaces sp-1/2/0 traceoptions flag all
set interfaces sp-1/2/0 services-options syslog host local services any
set interfaces sp-1/2/1 description bgf3_pgcp_service_ipv6
set interfaces sp-1/2/1 unit 0 family inet6
set interfaces sp-1/2/1 unit 10 family inet6
set interfaces sp-1/2/1 unit 10 service-domain inside
set interfaces sp-1/2/1 unit 20 family inet6
set interfaces sp-1/2/1 unit 20 service-domain outside
set interfaces sp-1/2/1 traceoptions flag all
set interfaces sp-1/2/1 services-options syslog host local services any
set services pgcp gateway bgf-1 gateway-address 172.16.10.1
set services pgcp gateway bgf-1 gateway-port 2944
set services pgcp gateway bgf-1 cleanup-timeout 3600
set services pgcp gateway bgf-2 gateway-address 172.16.20.2
set services pgcp gateway bgf-2 gateway-port 2944
set services pgcp gateway bgf-2 cleanup-timeout 3600
set services pgcp gateway bgf-3 gateway-address 172.16.30.3
set services pgcp gateway bgf-3 gateway-port 2944
set services pgcp gateway bgf-3 cleanup-timeout 3600
set services pgcp gateway bgf-1 gateway-controller gc-1 controller-address 33.0.0.1
set services pgcp gateway bgf-1 gateway-controller gc-1 controller-port 2944
set services pgcp gateway bgf-1 gateway-controller gc-1 interim-ah-scheme algorithm
    hmac-null
set services pgcp gateway bgf-2 gateway-controller gc-1 controller-address 33.0.0.1
set services pgcp gateway bgf-2 gateway-controller gc-1 controller-port 2944
set services pgcp gateway bgf-2 gateway-controller gc-1 interim-ah-scheme algorithm
    hmac-null
set services pgcp gateway bgf-3 gateway-controller gc-1 controller-address 33.0.0.1
set services pgcp gateway bgf-3 gateway-controller gc-1 controller-port 2944
set services pgcp gateway bgf-3 gateway-controller gc-1 interim-ah-scheme algorithm
    hmac-null
set services nat pool bgf1_peer_rtp-nat-pool-1 address 11.0.0.5
set services nat pool bgf1_peer_rtp-nat-pool-1 port automatic
set services nat pool bgf1_peer_rtp-nat-pool-1 pgcp
set services nat pool bgf1_peer_rtp-nat-pool-1 pgcp ports-per-session 2
set services nat pool bgf2_peer_rtp-nat-pool-2 address 11.0.0.25
set services nat pool bgf2_peer_rtp-nat-pool-2 port automatic
set services nat pool bgf2_peer_rtp-nat-pool-2 pgcp
```

```
set services nat pool bgf2_peer_rtp-nat-pool-2 pgcp ports-per-session 2
set services nat pool bgf3_peer_rtp-nat-pool-3 address 2001:db8:10:3::100/128
set services nat pool bgf3_peer_rtp-nat-pool-3 port automatic
set services nat pool bgf3_peer_rtp-nat-pool-3 pgcp
set services nat pool bgf3_peer_rtp-nat-pool-3 pgcp ports-per-session 2
set services nat pool bgf1_core_rtp-nat-pool-4 address 10.0.0.5
set services nat pool bgf1_core_rtp-nat-pool-4 port automatic
set services nat pool bgf1_core_rtp-nat-pool-4 pgcp
set services nat pool bgf1_core_rtp-nat-pool-4 pgcp ports-per-session 2
set services nat pool bgf2_core_rtp-nat-pool-5 address 10.0.0.25
set services nat pool bgf2_core_rtp-nat-pool-5 port automatic
set services nat pool bgf2_core_rtp-nat-pool-5 pgcp
set services nat pool bgf2_core_rtp-nat-pool-5 pgcp ports-per-session 4
set services nat pool bgf3_core_rtp-nat-pool-6 address 2001:db8:13:2::100/128
set services nat pool bgf3_core_rtp-nat-pool-6 port automatic
set services nat pool bgf3_core_rtp-nat-pool-6 pgcp
set services nat pool bgf3_core_rtp-nat-pool-6 pgcp ports-per-session 2
set services nat pool vgp1_peer_sip-nat-pool-7 address 11.0.0.2
set services nat pool vgp1_peer_sip-nat-pool-7 port range low 10000 high 50000
set services nat pool vgp1_peer_sip-nat-pool-7 pgcp
set services nat pool vgp1_peer_sip-nat-pool-7 pgcp remotely-controlled
set services nat pool vgp1_peer_sip-nat-pool-7 pgcp ports-per-session 2
set services nat pool bgf1_core_sip-nat-pool-8 address 10.0.0.2
set services nat pool bgf1_core_sip-nat-pool-8 port range low 10000 high 50000
set services nat pool bgf1_core_sip-nat-pool-8 pgcp
set services nat pool bgf1_core_sip-nat-pool-8 pgcp remotely-controlled
set services nat pool bgf1_core_sip-nat-pool-8 pgcp ports-per-session 2
set services pgcp media-service bgf1_peer_rtp_ms1 nat-pool bgf1_peer_rtp-nat-pool-1
set services pgcp media-service bgf1_core_rtp_ms4 nat-pool bgf1_core_rtp-nat-pool-4
set services pgcp media-service bgf1_peer_sip_ms7 nat-pool bgf1_peer_sip-nat-pool-7
set services pgcp media-service bgf1_core_sip_ms8 nat-pool bgf1_core_sip-nat-pool-8
set services pgcp media-service bgf2_peer_rtp_ms2 nat-pool bgf2_peer_rtp-nat-pool-2
set services pgcp media-service bgf2_core_rtp_ms5 nat-pool bgf2_core_rtp-nat-pool-5
set services pgcp media-service bgf3_peer_rtp_ms3 nat-pool bgf3_peer_rtp-nat-pool-3
set services pgcp media-service bgf3_core_rtp_ms6 nat-pool bgf3_core_rtp-nat-pool-6
set services pgcp virtual-interface 1 media-service bgf1_core_rtp_ms4
set services pgcp virtual-interface 1 media-service bgf1_core_sip_ms8
set services pgcp virtual-interface 1 media-service bgf2_core_rtp_ms5
set services pgcp virtual-interface 1 media-service bgf3_core_rtp_ms6
set services pgcp virtual-interface 2 media-service bgf1_peer_rtp_ms1
set services pgcp virtual-interface 2 media-service bgf1_peer_sip_ms7
set services pgcp virtual-interface 2 media-service bgf2_peer_rtp_ms2
set services pgcp virtual-interface 2 media-service bgf3_peer_rtp_ms3
set services pgcp rule bgf-rule1 gateway bgf-1 media-service bgf1_peer_rtp_ms1
set services pgcp rule bgf-rule1 gateway bgf-1 media-service bgf1_peer_sip_ms7
set services pgcp rule bgf-rule1 gateway bgf-1 media-service bgf1_core_rtp_ms4
set services pgcp rule bgf-rule1 gateway bgf-1 media-service bgf1_core_sip_ms8
set services pgcp rule bgf-rule2 gateway bgf-2 media-service bgf2_peer_rtp_ms2
set services pgcp rule bgf-rule2 gateway bgf-2 media-service bgf2_core_rtp_ms5
set services pgcp rule bgf-rule3 gateway bgf-3 media-service bgf3_peer_rtp_ms3
set services pgcp rule bgf-rule3 gateway bgf-3 media-service bgf3_core_rtp_ms6
set services stateful-firewall rule r1 match-direction input-output term t1 then reject
set services service-set bgf1-svc-set pgcp-rules bgf-rule1
set services service-set bgf1-svc-set stateful-firewall-rules r1
set services service-set bgf1-svc-set next-hop-service inside-service-interface
  sp-1/2/0.10
```

```
set services service-set bgf1-svc-set next-hop-service outside-service-interface
  sp-1/2/0.20
set services service-set bgf1-svc-set syslog host local-1 services any
set services service-set bgf2-svc-set pgcp-rules bgf-rule2
set services service-set bgf2-svc-set stateful-firewall-rules r1
set services service-set bgf2-svc-set next-hop-service inside-service-interface
  sp-1/2/0.30
set services service-set bgf2-svc-set next-hop-service outside-service-interface
  sp-1/2/0.40
set services service-set bgf2-svc-set syslog host local-1 services any
set services service-set bgf3-svc-set pgcp-rules bgf-rule3
set services service-set bgf3-svc-set stateful-firewall-rules r1
set services service-set bgf3-svc-set next-hop-service inside-service-interface
  sp-1/2/1.10
set services service-set bgf3-svc-set next-hop-service outside-service-interface
  sp-1/2/1.20
set services service-set bgf3-svc-set syslog host local-1 services any
set services pgcp gateway bgf-1 h248-properties diffserv default dscp 0x1D
```

Configuring the Service Interfaces

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

```
[edit interfaces]
set sp-1/2/0 description bgf1_bgf2_pgcp_service_ipv4
set sp-1/2/0 unit 0 family inet
set sp-1/2/0 unit 10 family inet
set sp-1/2/0 unit 10 service-domain inside
set sp-1/2/0 unit 20 family inet
set sp-1/2/0 unit 20 service-domain outside
set sp-1/2/0 unit 30 family inet
set sp-1/2/0 unit 30 service-domain inside
set sp-1/2/0 unit 40 family inet
set sp-1/2/0 unit 40 service-domain outside
set sp-1/2/0 traceoptions flag all
set sp-1/2/0 services-options syslog host local services any
set sp-1/2/1 description bgf3_pgcp_service_ipv6
set sp-1/2/1 unit 0 family inet6
set sp-1/2/1 unit 10 family inet6
set sp-1/2/1 unit 10 service-domain inside
set sp-1/2/1 unit 20 family inet6
set sp-1/2/1 unit 20 service-domain outside
set sp-1/2/1 traceoptions flag all
set sp-1/2/1 services-options syslog host local services any
```

Step-by-Step Procedure To configure the service interface:

1. Create the interface, and enter edit mode for the interface.

```
[edit interfaces]
user@sp-bgf-router#edit sp-1/2/0
```

2. Configure an IPv4 service interface for BGF–1 and BGF–2.

```
[edit interfaces sp-1/2/0]
```

```
user@sp-bgf-router#set description bgf1_bgf2_pgcp_service_ipv4
user@sp-bgf-router#set unit 0 family inet
user@sp-bgf-router#set unit 10 family inet
user@sp-bgf-router#set unit 10 service-domain inside
user@sp-bgf-router#set unit 20 family inet
user@sp-bgf-router#set unit 20 service-domain outside
user@sp-bgf-router#set unit 30 family inet
user@sp-bgf-router#set unit 30 service-domain inside
user@sp-bgf-router#set unit 40 family inet
user@sp-bgf-router#set unit 40 service-domain outside
user@sp-bgf-router#set traceoptions flag all
user@sp-bgf-router#set services-options syslog host local services any
```

3. Configure an IPv6 service interface for BGF–3.

```
[edit interfaces sp-1/2/1]
user@sp-bgf-router#set sp-1/2/1 description bgf3_pgcp_service_ipv6
user@sp-bgf-router#set sp-1/2/1 unit 0 family inet6
user@sp-bgf-router#set sp-1/2/1 unit 10 family inet6
user@sp-bgf-router#set sp-1/2/1 unit 10 service-domain inside
user@sp-bgf-router#set sp-1/2/1 unit 20 family inet6
user@sp-bgf-router#set sp-1/2/1 unit 20 service-domain outside
user@sp-bgf-router#set sp-1/2/1 traceoptions flag all
user@sp-bgf-router#set sp-1/2/1 services-options syslog host local services
  any
```

Configuration Results Display the results of the configuration.

```
[edit interfaces]
user@sp-bgf-router# show
sp-1/2/0 {
   description bgf1_bgf2_pgcp_service_ipv4;
   traceoptions {
      flag all;
   }
   services-options {
      syslog {
         host local {
            services any;
         }
      }
   }
   unit 0 {
      family inet;
   }
   unit 10 {
      family inet;
      service-domain inside;
   }
   unit 20 {
      family inet;
      service-domain outside;
   }
   unit 30 {
      family inet;
```

```
        service-domain inside;
    }
    unit 40 {
        family inet;
        service-domain outside;
    }
}
sp-1/2/1 {
    description bgf3_pgcp_service_ipv6;
    traceoptions {
        flag all;
    }
    services-options {
        syslog {
            host local {
                services any;
            }
        }
    }
    unit 0 {
        family inet6;
    }
    unit 10 {
        family inet6;
        service-domain inside;
    }
    unit 20 {
        family inet6;
        service-domain outside;
    }
}
```

Configuring the Virtual BGFs

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

```
[edit services pgcp]
set gateway bgf-1 gateway-address 172.16.10.1
set gateway bgf-1 gateway-port 2944
set gateway bgf-1 cleanup-timeout 3600
set gateway bgf-1 gateway-controller gc-1 controller-address 33.0.0.1
set gateway bgf-1 gateway-controller gc-1 controller-port 2944
set gateway bgf-1 gateway-controller gc-1 interim-ah-scheme algorithm hmac-null
set gateway bgf-2 gateway-address 172.16.20.2
set gateway bgf-2 gateway-port 2944
set gateway bgf-2 cleanup-timeout 3600
set gateway bgf-2 gateway-controller gc-1 controller-address 33.0.0.1
set gateway bgf-2 gateway-controller gc-1 controller-port 2944
set gateway bgf-2 gateway-controller gc-1 interim-ah-scheme algorithm hmac-null
set gateway bgf-3 gateway-address 172.16.30.3
set gateway bgf-3 gateway-port 2944
set gateway bgf-3 cleanup-timeout 3600
set gateway bgf-3 gateway-controller gc-1 controller-address 33.0.0.1
set gateway bgf-3 gateway-controller gc-1 controller-port 2944
```

set gateway bgf-3 gateway-controller gc-1 interim-ah-scheme algorithm hmac-null

Step-by-Step Procedure To configure the virtual BGFs:

1. Configure BGF-1.

```
[edit services pgcp]
user@sp-bgf-router#edit gateway bgf-1

[edit services pgcp gateway bgf-1]
user@sp-bgf-router#set gateway-address 172.16.10.1
user@sp-bgf-router#set gateway-port 2944
user@sp-bgf-router#set cleanup-timeout 3600
user@sp-bgf-router#set gateway-controller gc-1 controller-address 33.0.0.1
user@sp-bgf-router#set gateway-controller gc-1 controller-port 2944
user@sp-bgf-router#set gateway-controller gc-1 interim-ah-scheme algorithm
  hmac-null
```

2. Configure BGF-2.

```
[edit services pgcp]
user@sp-bgf-router#edit gateway bgf-2

[edit services pgcp gateway bgf-2]
user@sp-bgf-router#set gateway-address 172.16.20.2
user@sp-bgf-router#set gateway-port 2944
user@sp-bgf-router#set cleanup-timeout 3600
user@sp-bgf-router#set gateway-controller gc-1 controller-address 33.0.0.1
user@sp-bgf-router#set gateway-controller gc-1 controller-port 2944
user@sp-bgf-router#set gateway-controller gc-1 interim-ah-scheme algorithm
  hmac-null
```

3. Configure BGF-3.

```
[edit services pgcp]
user@sp-bgf-router#edit gateway bgf-3

[edit services pgcp gateway bgf-3]
user@sp-bgf-router#set gateway-address 172.16.30.3
user@sp-bgf-router#set gateway-port 2944
user@sp-bgf-router#set cleanup-timeout 3600
user@sp-bgf-router#set gateway-controller gc-1 controller-address 33.0.0.1
user@sp-bgf-router#set gateway-controller gc-1 controller-port 2944
user@sp-bgf-router#set gateway-controller gc-1 interim-ah-scheme algorithm
  hmac-null
```

Configuration Results Display the results of the configuration.

```
[edit services pgcp]
user@sp-bgf-router# show
gateway bgf-1 {
   gateway-address 172.16.10.1;
   gateway-port 2944;
   cleanup-timeout 3600;
   gateway-controller gc-1 {
```

```
        controller-address 33.0.0.1;
        controller-port 2944;
        interim-ah-scheme {
            algorithm hmac-null;
        }
    }
    }
    gateway bgf-2 {
        gateway-address 172.16.20.2;
        gateway-port 2944;
        cleanup-timeout 3600;
        gateway-controller gc-1 {
            controller-address 33.0.0.1;
            controller-port 2944;
            interim-ah-scheme {
                algorithm hmac-null;
            }
        }
    }
    gateway bgf-3 {
        gateway-address 172.16.30.3;
        gateway-port 2944;
        cleanup-timeout 3600;
        gateway-controller gc-1 {
            controller-address 33.0.0.1;
            controller-port 2944;
            interim-ah-scheme {
                algorithm hmac-null;
            }
        }
    }
## Warning: missing mandatory statement(s): 'virtual-interface'
```

Configuring NAT Pools

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

```
[edit services nat]
set pool bgf1_peer_rtp-nat-pool-1 address 11.0.0.5
set pool bgf1_peer_rtp-nat-pool-1 port automatic
set pool bgf1_peer_rtp-nat-pool-1 pgcp
set pool bgf1_peer_rtp-nat-pool-1 pgcp ports-per-session 2
set pool bgf2_peer_rtp-nat-pool-2 address 11.0.0.25
set pool bgf2_peer_rtp-nat-pool-2 port automatic
set pool bgf2_peer_rtp-nat-pool-2 pgcp
set pool bgf2_peer_rtp-nat-pool-2 pgcp ports-per-session 2
set pool bgf3_peer_rtp-nat-pool-3 address 2001:db8:10:3::100/128
set pool bgf3_peer_rtp-nat-pool-3 port automatic
set pool bgf3_peer_rtp-nat-pool-3 pgcp
set pool bgf3_peer_rtp-nat-pool-3 pgcp ports-per-session 2
set pool bgf1_core_rtp-nat-pool-4 address 10.0.0.5
set pool bgf1_core_rtp-nat-pool-4 port automatic
set pool bgf1_core_rtp-nat-pool-4 pgcp
set pool bgf1_core_rtp-nat-pool-4 pgcp ports-per-session 2
```

```
set pool bgf2_core_rtp-nat-pool-5 address 10.0.0.25
set pool bgf2_core_rtp-nat-pool-5 port automatic
set pool bgf2_core_rtp-nat-pool-5 pgcp
set pool bgf2_core_rtp-nat-pool-5 pgcp ports-per-session 4
set pool bgf3_core_rtp-nat-pool-6 address 2001:db8:13:2::100/128
set pool bgf3_core_rtp-nat-pool-6 port automatic
set pool bgf3_core_rtp-nat-pool-6 pgcp
set pool bgf3_core_rtp-nat-pool-6 pgcp ports-per-session 2
set pool vgp1_peer_sip-nat-pool-7 address 11.0.0.2
set pool vgp1_peer_sip-nat-pool-7 port range low 10000 high 50000
set pool vgp1_peer_sip-nat-pool-7 pgcp
set pool vgp1_peer_sip-nat-pool-7 pgcp remotely-controlled
set pool vgp1_peer_sip-nat-pool-7 pgcp ports-per-session 2
set pool bgf1_core_sip-nat-pool-8 address 10.0.0.2
set pool bgf1_core_sip-nat-pool-8 port range low 10000 high 50000
set pool bgf1_core_sip-nat-pool-8 pgcp
set pool bgf1_core_sip-nat-pool-8 pgcp remotely-controlled
set pool bgf1_core_sip-nat-pool-8 pgcp ports-per-session 2
```

Step-by-Step Procedure To configure NAT pools:

1. Create a media (RTP) NAT pool for BGF-1 for the access (peering) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf1_peer_rtp-nat-pool-1

[edit services nat pool bgf1_peer_rtp-nat-pool-1]
user@sp-bgf-router#set address 11.0.0.5
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pool pg1_peer_rtp-nat-pool-1 pgcp ports-per-session 2
```

2. Create a media (RTP) NAT pool for BGF-2 for the access (peering) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf2_peer_rtp-nat-pool-2

[edit services nat pool bgf2_peer_rtp-nat-pool-2]
user@sp-bgf-router#set address 11.0.0.25
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pgcp ports-per-session 2
```

3. Create a media (RTP) NAT pool for BGF-3 for the access (peering) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf3_peer_rtp-nat-pool-3

[edit services nat pool bgf3_peer_rtp-nat-pool-3]
user@sp-bgf-router#set address 2001:db8:10:3::100/128
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
```

```
user@sp-bgf-router#set pgcp ports-per-session 2
```

4. Create a media (RTP) NAT pool for BGF-1 for the backbone (service provider) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf1_core_rtp-nat-pool-4

[edit services nat pool bgf1_core_rtp-nat-pool-4]
user@sp-bgf-router#set address 10.0.0.5
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pgcp ports-per-session 2
```

5. Create a media (RTP) NAT pool for BGF-2 for the backbone (service provider) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf2_core_rtp-nat-pool-5

[edit services nat pool bgf2_core_rtp-nat-pool-5]
user@sp-bgf-router#set address 10.0.0.25
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set ports-per-session 4
```

6. Create a media (RTP) NAT pool for BGF-3 for the backbone (service provider) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool bgf3_core_rtp-nat-pool-6

[edit services nat pool bgf3_core_rtp-nat-pool-6]
user@sp-bgf-router#set address 2001:db8:13:2::100/128
user@sp-bgf-router#set port automatic
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pgcp ports-per-session 2
```

7. Configure a signaling (SIP) NAT pool for BGF-1 for the access (peering) side of the network.

```
[edit services nat]
user@sp-bgf-router#edit pool vgp1_peer_sip-nat-pool-7

[edit services nat pool vgp1_peer_sip-nat-pool-7]
user@sp-bgf-router#set address 11.0.0.2
user@sp-bgf-router#set port range low 10000 high 50000
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pgcp remotely-controlled
user@sp-bgf-router#set ports-per-session 2
```

8. Configure a signaling (SIP) NAT pool for the backbone (service provider) side of the network.

```
[edit services nat]
```

```
user@sp-bgf-router#edit pool bgf1_core_sip-nat-pool-8

[edit services nat pool bgf1_core_sip-nat-pool-8]
user@sp-bgf-router#set address 10.0.0.2
user@sp-bgf-router#set port range low 10000 high 50000
user@sp-bgf-router#set pgcp
user@sp-bgf-router#set pgcp remotely-controlled
user@sp-bgf-router#set pgcp ports-per-session 2
```

Configuration Results Display the results of the configuration.

```
[edit services nat]
user@sp-bgf-router# show
pool bgf1_peer_rtp-nat-pool-1 {
    pgcp {
        ports-per-session 2;
    }
    address 11.0.0.5/32;
    port automatic;
}
    pool bgf2_peer_rtp-nat-pool-2 {
        pgcp {
            ports-per-session 2;
        }
        address 11.0.0.25/32;
        port automatic;
    }
    pool bgf3_peer_rtp-nat-pool-3 {
        pgcp {
            ports-per-session 2;
        }
        address 2001:db8:10:3::100/128;
        port automatic;
    }
    pool bgf1_core_rtp-nat-pool-4 {
        pgcp {
            ports-per-session 2;
        }
        address 10.0.0.5/32;
        port automatic;
    }
    pool bgf2_core_rtp-nat-pool-5 {
        pgcp {
            ports-per-session 4;
        }
        address 10.0.0.25/32;
        port automatic;
    }
    pool bgf3_core_rtp-nat-pool-6 {
        pgcp {
            ports-per-session 2;
        }
        address 2001:db8:13:2::100/128;
        port automatic;
    }
```

```
pool vgp1_peer_sip-nat-pool-7 {
   pgcp {
      remotely-controlled;
      ports-per-session 2;
   }
   address 11.0.0.2/32;
   port range low 10000 high 50000;
}
pool bgf1_core_sip-nat-pool-8 {
   pgcp {
      remotely-controlled;
      ports-per-session 2;
   }
   address 10.0.0.2/32;
   port range low 10000 high 50000;
}
```

Assigning the NAT Pools to a Media Service

CLI Quick Configuration To quickly create media services and assign NAT pools to a media service, copy the following commands and paste them into the router terminal window:

```
[edit services pgcp]
set media-service bgf1_peer_rtp_ms1 nat-pool bgf1_peer_rtp-nat-pool-1
set media-service bgf1_core_rtp_ms4 nat-pool bgf1_core_rtp-nat-pool-4
set media-service bgf1_peer_sip_ms7 nat-pool bgf1_peer_sip-nat-pool-7
set media-service bgf1_core_sip_ms8 nat-pool bgf1_core_sip-nat-pool-8
set media-service bgf2_peer_rtp_ms2 nat-pool bgf2_peer_rtp-nat-pool-2
set media-service bgf2_core_rtp_ms5 nat-pool bgf2_core_rtp-nat-pool-5
set media-service bgf3_peer_rtp_ms3 nat-pool bgf3_peer_rtp-nat-pool-3
set media-service bgf3_core_rtp_ms6 nat-pool bgf3_core_rtp-nat-pool-6
```

Step-by-Step Procedure To configure a media service:

1. Configure media services for each of the NAT pools for BGF-1.

```
[edit services pgcp]
user@sp-bgf-router#set media-service bgf1_peer_rtp_ms1 nat-pool
   bgf1_peer_rtp-nat-pool-1
user@sp-bgf-router#set media-service bgf1_core_rtp_ms4 nat-pool
   bgf1_core_rtp-nat-pool-4
user@sp-bgf-router#set media-service bgf1_peer_sip_ms7 nat-pool
   vgp1_peer_sip-nat-pool-7
user@sp-bgf-router#set media-service bgf1_core_sip_ms8 nat-pool
   bgf1_core_sip-nat-pool-8
```

2. Configure a media service for each of the NAT pools for BGF-2.

```
[edit services pgcp]
user@sp-bgf-router#set media-service bgf2_peer_rtp_ms2 nat-pool
   bgf2_peer_rtp-nat-pool-2
user@sp-bgf-router#set media-service bgf2_core_rtp_ms5 nat-pool
   bgf2_core_rtp-nat-pool-5
```

3. Configure media services for each of the NAT pools for BGF-3.

```
[edit services pgcp]
user@sp-bgf-router#set media-service bgf3_peer_rtp_ms3 nat-pool
   bgf3_peer_rtp-nat-pool-3
user@sp-bgf-router#set media-service bgf3_core_rtp_ms6 nat-pool
   bgf3_core_rtp-nat-pool-6
```

Configuration Results Display the results of the configuration.

```
[edit services pgcp]
user@sp-bgf-router#show
...
media-service bgf1_peer_rtp_ms1 {
   nat-pool bgf1_peer_rtp-nat-pool-1;
   }
   media-service bgf1_core_rtp_ms4 {
      nat-pool bgf1_core_rtp-nat-pool-4;
   }
   media-service bgf2_peer_rtp_ms2 {
      nat-pool bgf2_peer_rtp-nat-pool-2;
   }
   media-service bgf2_core_rtp_ms5 {
      nat-pool bgf2_core_rtp-nat-pool-5;
   }
   media-service bgf3_peer_rtp_ms3 {
      nat-pool bgf3_peer_rtp-nat-pool-3;
   }
   media-service bgf3_core_rtp_ms6 {
      nat-pool bgf3_core_rtp-nat-pool-6;
   }
   media-service bgf1_peer_sip_ms7 {
      nat-pool bgf1_peer_sip-nat-pool-7;
   }
   media-service bgf1_core_sip_ms8 {
      nat-pool bgf1_core_sip-nat-pool-8;
   }
## Warning: missing mandatory statement(s): 'virtual-interface'
```

Configuring the Virtual Interfaces

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

```
[edit services pgcp]
set virtual-interface 1 media-service bgf1_core_rtp_ms4
set virtual-interface 1 media-service bgf1_core_sip_ms8
set virtual-interface 1 media-service bgf2_core_rtp_ms5
set virtual-interface 1 media-service bgf3_core_rtp_ms6
set virtual-interface 2 media-service bgf1_peer_rtp_ms1
set virtual-interface 2 media-service bgf1_peer_sip_ms7
set virtual-interface 2 media-service bgf2_peer_rtp_ms2
set virtual-interface 2 media-service bgf3_peer_rtp_ms3
```

Step-by-Step Procedure To configure a virtual interface:

1. Create a virtual interface for the backbone (service provider) side of the network. Specify the names of the media services that contains the NAT pool to be used for gates on the virtual interface that you are configuring.

```
[edit services pgcp]
edit virtual-interface 1
```

```
[edit services pgcp virtual-interface 1]
user@sp-bgf-router#set media-service bgf1_core_rtp_ms4
user@sp-bgf-router#set media-service bgf1_core_sip_ms8
user@sp-bgf-router#set media-service bgf2_core_rtp_ms5
user@sp-bgf-router#set media-service bgf3_core_rtp_ms6
```

2. Create a virtual interface for the access (peering) side of the network. Specify the names of the media services that contains the NAT pool to be used for gates on the virtual interface that you are configuring.

```
[edit services pgcp]
edit virtual-interface 2
```

```
[edit services pgcp virtual-interface 2]
user@sp-bgf-router#set media-service bgf1_peer_rtp_ms1
user@sp-bgf-router#set media-service bgf1_peer_sip_ms7
user@sp-bgf-router#set media-service bgf2_peer_rtp_ms2
user@sp-bgf-router#set media-service bgf3_peer_rtp_ms3
```

Configuration Results Display the results of the configuration.

```
[edit services pgcp virtual-interface 1]
user@sp-bgf-router# show
virtual-interface 1 {
   media-service [ bgf1_core_rtp_ms4 bgf1_core_sip_ms8 bgf2_core_rtp_ms5
      bgf3_core_rtp_ms6 ];
}
   virtual-interface 2 {
      media-service [ bgf1_peer_rtp_ms1 bgf1_peer_sip_ms7 bgf2_peer_rtp_ms2
         bgf3_peer_rtp_ms3 ];
   }
```

Configuring Rules for the BGF

You define rules that specify the NAT pool (media service) used on a specific virtual BGF.

CLI Quick Configuration To quickly define the rules, copy the following commands and paste them into the router terminal window:

```
[edit services pgcp]
set rule bgf-rule1 gateway bgf-1 media-service bgf1_peer_rtp_ms1
set rule bgf-rule1 gateway bgf-1 media-service bgf1_peer_sip_ms7
set rule bgf-rule1 gateway bgf-1 media-service bgf1_core_rtp_ms4
set rule bgf-rule1 gateway bgf-1 media-service bgf1_core_sip_ms8
set rule bgf-rule2 gateway bgf-2 media-service bgf2_peer_rtp_ms2
```

```
set rule bgf-rule2 gateway bgf-2 media-service bgf2_core_rtp_ms5
set rule bgf-rule3 gateway bgf-3 media-service bgf3_peer_rtp_ms3
set rule bgf-rule3 gateway bgf-3 media-service bgf3_core_rtp_ms6
```

Step-by-Step Procedure To configure the rules for the BGF:

1. Create a rule for BGF-1, and specify the media services that contains the NAT pools to be used for this virtual BGF.

```
[edit services pgcp]
user@sp-bgf-router#edit rule bgf-rule1

[edit services pgcp rule bgf-rule1]
user@sp-bgf-router#set gateway bgf-1
user@sp-bgf-router#set media-service bgf1_peer_rtp_ms1
user@sp-bgf-router#set media-service bgf1_peer_sip_ms7
user@sp-bgf-router#set media-service bgf1_core_rtp_ms4
user@sp-bgf-router#set media-service bgf1_core_sip_ms8
```

2. Create a rule for BGF-2, and specify the media services that contains the NAT pools to be used for this virtual BGF.

```
[edit services pgcp]
user@sp-bgf-router#edit rule bgf-rule2

[edit services pgcp rule bgf-rule2]
user@sp-bgf-router#set gateway bgf-2
user@sp-bgf-router#set media-service bgf2_peer_rtp_ms2
user@sp-bgf-router#set media-service bgf2_core_rtp_ms5
```

3. Create a rule for BGF-3, and specify the media services that contains the NAT pools to be used for this virtual BGF.

```
[edit services pgcp]
user@sp-bgf-router#edit rule bgf-rule3

[edit services pgcp rule bgf-rule3]
user@sp-bgf-router#set gateway bgf-3
set rule bgf-rule3 gateway bgf-3 media-service bgf3_peer_rtp_ms3
set rule bgf-rule3 gateway bgf-3 media-service bgf3_core_rtp_ms6
```

Configuration Results Display the results of the configuration.

```
[edit services pgcp]
user@sp-bgf-router# show
. . .
rule bgf-rule1 {
   gateway bgf-1;
   media-service [ bgf1_peer_rtp_ms1 bgf1_peer_sip_ms7 bgf1_core_rtp_ms4
      bgf1_core_sip_ms8 ];
}
   rule bgf-rule2 {
      gateway bgf-2;
      media-service [ bgf2_peer_rtp_ms2 bgf2_core_rtp_ms5 ];
```

```
}
rule bgf-rule3 {
    gateway bgf-3;
    media-service [ bgf3_peer_rtp_ms3 bgf3_core_rtp_ms6 ];
}
```

Configuring a Stateful Firewall

You define rules that specify the NAT pool (media service) used on a specific virtual BGF.

CLI Quick Configuration To quickly define the rules, copy the following commands and paste them into the router terminal window:

```
[edit services stateful-firewall]
set rule r1 match-direction input-outputset rule r1 term t1 then reject
```

Step-by-Step Procedure To create a stateful firewall:

1. Create a stateful firewall rule.

```
[edit services stateful-firewall]
user@host#edit rule r1
```

2. Set the match direction for the rule.

```
[edit services stateful-firewall rule r1]
user@host#set match-direction input-output
```

3. Add a term to the rule with the action set to reject.

```
[edit services stateful-firewall rule r1]
user@host#set term t1 then reject
```

Configuration Results Display the results of the configuration.

```
[edit services stateful-firewall]
user@sp-bgf-router# show
rule r1 {
    match-direction input-output;
    term t1 {
        then {
            reject;
        }
    }
}
```

Configuring a Service Set

CLI Quick Configuration To quickly define a service set, copy the following commands and paste them into the router terminal window:

```
[edit services]
set service-set bgf1-svc-set pgcp-rules bgf-rule1
```

```
set service-set bgf1-svc-set stateful-firewall-rules r1
set service-set bgf1-svc-set next-hop-service inside-service-interface sp-1/2/0.10
set service-set bgf1-svc-set next-hop-service outside-service-interface sp-1/2/0.20
set service-set bgf1-svc-set syslog host local-1 services any
set service-set bgf2-svc-set pgcp-rules bgf-rule2
set service-set bgf2-svc-set stateful-firewall-rules r1
set service-set bgf2-svc-set next-hop-service inside-service-interface sp-1/2/0.30
set service-set bgf2-svc-set next-hop-service outside-service-interface sp-1/2/0.40
set service-set bgf2-svc-set syslog host local-1 services any
set service-set bgf3-svc-set pgcp-rules bgf-rule3
set service-set bgf3-svc-set stateful-firewall-rules r1
set service-set bgf3-svc-set next-hop-service inside-service-interface sp-1/2/1.10
set service-set bgf3-svc-set next-hop-service outside-service-interface sp-1/2/1.20
set service-set bgf3-svc-set syslog host local-1 services any
```

Step-by-Step Procedure To configure the service sets:

1. Configure a service set for bgf-1.

```
[edit services]
user@sp-bgf-router#edit service-set bgf1-svc-set

[edit services service-set bgf1-svc-set]
user@sp-bgf-router#set pgcp-rules bgf-rule1
user@sp-bgf-router#set stateful-firewall-rules r1
user@sp-bgf-router#set next-hop-service inside-service-interface sp-1/2/0.10
user@sp-bgf-router#set next-hop-service outside-service-interface sp-1/2/0.20
user@sp-bgf-router#set syslog host local-1 services any
```

2. Configure a service set for BGF-2.

```
[edit services]
user@sp-bgf-router#edit service-set bgf2-svc-set

[edit services service-set bgf2-svc-set]
user@sp-bgf-router#set pgcp-rules bgf-rule2
user@sp-bgf-router#set stateful-firewall-rules r1
user@sp-bgf-router#set next-hop-service inside-service-interface sp-1/2/0.30
user@sp-bgf-router#set next-hop-service outside-service-interface sp-1/2/0.40
user@sp-bgf-router#set syslog host local-1 services any
```

3. Configure a service set for BGF-3.

```
[edit services]
user@sp-bgf-router#edit service-set bgf3-svc-set

[edit services service-set bgf3-svc-set]
user@sp-bgf-router#set pgcp-rules bgf-rule3
user@sp-bgf-router#set stateful-firewall-rules r1
user@sp-bgf-router#set next-hop-service inside-service-interface sp-1/2/1.10
user@sp-bgf-router#set next-hop-service outside-service-interface sp-1/2/1.20
user@sp-bgf-router#set syslog host local-1 services any
```

Configuration Results Display the results of the configuration.

```
[edit services]
user@sp-bgf-router# show service-set bgf1-svc-set
syslog {
    host local-1 {
        services any;
    }
}
stateful-firewall-rules r1;
pgcp-rules bgf-rule1;
next-hop-service {
    inside-service-interface sp-1/2/0.10;
    outside-service-interface sp-1/2/0.20;
}

[edit services]
user@sp-bgf-router# show service-set bgf2-svc-set
syslog {
    host local-1 {
        services any;
        }
    }
stateful-firewall-rules r1;
pgcp-rules bgf-rule2;
next-hop-service {
    inside-service-interface sp-1/2/0.30;
    outside-service-interface sp-1/2/0.40;
}

[edit services]
user@sp-bgf-router# show service-set bgf3-svc-set
syslog {
    host local-1 {
        services any;
        }
    }
stateful-firewall-rules r1;
pgcp-rules bgf-rule3;
next-hop-service {
    inside-service-interface sp-1/2/1.10;
    outside-service-interface sp-1/2/1.20;
}
```

Configuring QoS for Voice Calls

CLI Quick Configuration To quickly configure a default value for the Differentiated Services (DiffServ) code point (DSCP), copy the following command and paste it into the router terminal window:

```
[edit services pgcp]
set gateway bgf-1 h248-properties diffserv dscp default 0x1D
```

Step-by-Step Procedure To configure default values for H.248 DiffServ properties:

1. Access the configuration of the H.248 DiffServ properties.

```
[edit services pgcp gateway bgf-1]
```

```
user@sp-bgf-router#edit h248-properties diffserv
```

2. Configure a value for the DSCP.

```
[edit services pgcp gateway bgf-1 h248-properties diffserv]
user@sp-bgf-router#set dscp default 0x1D
```

Configuration Results Display the results of the configuration.

```
[edit services pgcp gateway bgf-1 h248-properties diffserv]
user@sp-bgf-router# show
dscp { default 0x1D;
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the Active BGF Configuration on page 173
- Verifying That Gates Are Running on page 176
- Verifying Terminations on page 177
- Verifying PGCP Flows on page 177
- Verifying H.248 Parameters Set by the Gateway Controller on page 178

Verifying the Active BGF Configuration

Purpose Verify the active BGF configuration that is running on your router.

Action

```
user@sp-bgf-router> show services pgcp active-configuration gateway *
Packet gateway media service configuration:
 Media service name: bgf1_peer_rtp_ms1
  Nat pool             :  bgf1_peer_rtp-nat-pool-1

Packet gateway media service configuration:
 Media service name: bgf2_peer_rtp_ms2
  Nat pool             :  bgf2_peer_rtp-nat-pool-2

Packet gateway media service configuration:
 Media service name: bgf3_peer_rtp_ms3
  Nat pool             :  bgf3_peer_rtp-nat-pool-3

Packet gateway media service configuration:
 Media service name: bgf1_core_rtp_ms4
  Nat pool             :  bgf1_core_rtp-nat-pool-4

Packet gateway media service configuration:
 Media service name: bgf2_core_rtp_ms5
  Nat pool             :  core_rtp-nat-pool-5

Packet gateway media service configuration:
 Media service name:  bgf3_core_rtp_ms6
  Nat pool             :  bgf3_core_rtp-nat-pool-6

Packet gateway media service configuration:
 Media service name: bgf1_peer_sip_ms7
```

```
  Nat pool             :  bgf1_peer_sip-nat-pool-7

Packet gateway media service configuration:
 Media service name: bgf1_core_sip_ms8
  Nat pool             :  bgf1_core_sip-nat-pool-8

 Packet gateway virtual interface configuration:
  Virtual Interface name: 1
  Status               :  In-Service
  Media Service Name   :  bgf1_core_rtp_ms4
  Media Service Name   :  bgf1_core_sip_ms8
  Media Service Name   :  bgf2_core_rtp_ms5
  Media Service Name   :  bgf2_core_rtp_ms5

 Packet gateway virtual interface configuration:
  Virtual Interface name: 2
  Status               :  In-Service
  Media Service Name   :  bgf1_peer_rtp_ms1
  Media Service Name   :  bgf1_peer_sip_ms7
  Media Service Name   :  bgf2_peer_rtp_ms2
  Media Service Name   :  bgf3_peer_rtp_ms3

Virtual BGF configuration:
  Name                                    :  bgf-1
  IP address                              :  172.16.10.1
  Port                                    :  2944
  Status                                  :  In-Service (Registered)
  Active gateway controller               :  gc-1
  Replication socket                      :  Connected (Syncing)
  Cleanup timeout [secs]                  :  3600
  Gate inactivity delay [secs]            :  240
  Gate inactivity duration (Q-MI ) [secs]  :  86400
  Latching Deadlock duration [secs]       : 15

Virtual BGF configuration:
  Name                                    :  bgf-2
  IP address                              :  172.16.20.2
  Port                                    :  2944
  Status                                  :  In-Service (Disconnected)
  Active gateway controller               :
  Replication socket                      :  Connected (Syncing)
  Cleanup timeout [secs]                  :  3600
  Gate inactivity delay [secs]            :  240
  Gate inactivity duration (Q-MI ) [secs]  :  86400
  Latching Deadlock duration [secs]       : 15

Virtual BGF configuration:
  Name                                    :  bgf-3
  IP address                              :  172.16.30.3
  Port                                    :  2944
  Status                                  :  In-Service (Disconnected)
  Active gateway controller               :
  Replication socket                      :  Connected (Syncing)
  Cleanup timeout [secs]                  :  3600
  Gate inactivity delay [secs]            :  240
  Gate inactivity duration (Q-MI ) [secs]  :  86400
  Latching Deadlock duration [secs]       : 15

H248 timers configuration:
 Max waiting delay (MWD) [millisec]          :  10000
 Max retransmission delay (T-MAX) [millisec] :  25000
```

```
 Initial average ack delay (I-AAD) [millisec]:  1000
 Max net propagation delay (M-NPD) [millisec]:  5000

H248 options configuration:
 Wildcard response service-change        :  NO

H248 diffserv configuration:
 dscp          :  0x00

H248 segmentation        :               minimum        maximum        default
  MG segmentation timer [millisec]         :  500          30000          4000
  MG maximum PDU size [bytes]              :  512          65507          1472
  MGC segmentation timer [millisec]        :  500          30000          4000
  MGC maximum PDU size [bytes]             :  512          65507          1472

H248 base root           :                    minimum     maximum      default
  Normal MG execution time [millisec]      :  500           29000          500
  MG Provisional response timer [millisec] :  500           30000         2000
  MG Originated pending limit              :  1               512            4
  Normal MGC execution time [millisec]     :  500           29000          500
  MGC Provisional response timer [millisec]:  500           30000         4000
  MGC Originated pending limit             :  1               512            4

Fast update filters:
 Maximum terms              : 20000
 Maximum term percentage    : 10

Packet gateway controller configuration:
 Controller name                  :  gc-1
 Controller IP address            :  33.0.0.1
 Controller port                  :  2944

Packet gateway rule configuration:
 Rule name            :  bgf-rule1
 Gateway name         :  bgf-1

Packet gateway rule configuration:
 Rule name            :  bgf-rule2
 Gateway name         :  bgf-2

Packet gateway rule configuration:
 Rule name            :  bgf-rule3
 Gateway name         :  bgf-3

Packet gateway service set configuration:
 Service set name     :  bgf1-svc-set
 Service set id       :  1
 Rule name            :  bgf-rule1

Packet gateway service set configuration:
 Service set name     :  bgf2-svc-set
 Service set id       :  2
 Rule name            :  bgf-rule2

Packet gateway service set configuration:
 Service set name     :  bgf3-svc-set
 Service set id       :  3
 Rule name            :  bgf-rule3

Packet gateway service pics status:
 Name    : sp-1/2/0
```

```
 Status  : Connected

Packet gateway service pics status:
 Name    : sp-1/2/1
 Status  : Connected

Firewall:
 Status             :  Connected
 Number of terms    :  2
 Number of filters  :  2
```

Meaning Use the show services pgcp active-configuration command to see your configuration and to display the current status of your virtual interfaces, virtual BGF, and services interfaces.

In addition, make sure that:

- At least one virtual BGF is In-Service (Registered). Virtual BGF Out-Of-Service might mean that:
  - The gateway controller is down.
  - The network connection between the gateway controller and the BGF is down, or there is a related network problem.
  - An unknown software problem exists. In this case, review the BGF logs for more information or contact JTAC.
- The Replication socket is Connected. If it is not, graceful Routing Engine switchover (GRES) is not enabled.
- The BGF service interface status is Connected. If it is not, there might be a hardware problem with the interface.
- The Firewall Status is Connected. If it is not, no connection exists to the fast update filters for rate limiting.

Verifying That Gates Are Running

Purpose Verify that gates are running on bgf-1.

Action

```
user@sp-bgf-router> show services pgcp gates gateway bgf-1
Virtual BGF configuration:
  Name                                  :  bgf-1
  IP address                            :  172.16.10.1
  Port                                  :  2944
  Status                                :  In-Service (Registered)

Gate information:
Gate id: 4295033088
Gate state:  active
Action: forward
Service set id: 1
Media card: sp-1/2/0
Media handler: bgf1-svc-set
Termination-id-string: ip/4/vif-0/2

Gate id: 4295033089
```

```
Gate state:  active
Action: forward
Service set id: 1
Media card: sp-1/2/0
Media handler: bgf1-svc-set
Termination-id-string: ip/4/vif-0/3
```

Meaning The show services pgcp gates command lists the gates on the virtual BGF. It shows whether gates are active, disabled, or closed. It also shows the current action being performed on the gate—forward, add, or drop.

Verifying Terminations

Purpose Verify the terminations on bgf-1.

Action

```
user@sp-bgf-router> show services pgcp terminations gateway bgf-1
Virtual BGF configuration:
  Name                                  :  bgf-1
  IP address                            :  172.16.10.1
  Port                                  :  2944
  Status                                :  In-Service (Registered)


Termination name                    State           Duration(msecs)
ip/4/vif-0/2       In-service       390288
Gate-id         Direction       State        Action
4295033088      A->B            active       forward
4295033089      B->A            active       forward


Termination name                    State           Duration(msecs)
ip/4/vif-0/3       In-service       390294
Gate-id         Direction       State        Action
4295033088      A->B            active       forward
4295033089      B->A            active       forward
```

Meaning The show services pgcp terminations command lists the terminations on the virtual BGF. It shows whether the gates within a termination are active, disabled, or closed. You can use the termination names (termination IDs) to troubleshoot problems with voice calls.

Verifying PGCP Flows

Purpose Verify the PGCP flows.

Action

```
user@sp-bgf-router> show services pgcp flows gateway bgf-1
Interface: sp-1/2/0, Service set: bgf1-svc-set
Flow                                                 State    Dir       Frm count
Gate id: 4295033089
UDP            20.0.0.1:0     ->    11.0.0.5:1024  Forward  I              0
    NAT source         20.0.0.1:0       ->     10.10.0.5:1024
    NAT dest       11.0.0.5:1024    ->         10.0.0.1:20002
Gate id: 4295033089
UDP            20.0.0.1:0     ->    11.0.0.5:1025  Forward  I              0
    NAT source         20.0.0.1:0       ->     10.10.0.5:1025
    NAT dest       11.0.0.5:1025    ->         10.0.0.1:20003
```

```
Gate id: 4295033088
UDP            0.0.0.0:0     ->    10.10.0.5:1024  Forward  I              0
    NAT source         0.0.0.0:0       ->     11.0.0.5:1024
    NAT dest       10.10.0.5:1024    ->         20.0.0.1:10002
Gate id: 4295033088
UDP            0.0.0.0:0     ->    10.10.0.5:1025  Forward  I              0
    NAT source         0.0.0.0:0       ->     11.0.0.5:1025
    NAT dest       10.10.0.5:1025    ->         20.0.0.1:10003
```

Verifying H.248 Parameters Set by the Gateway Controller

Purpose Verify the H.248 parameters that are set by the gateway controller.

Action

```
user@sp-bgf-router> show services pgcp terminations gateway bgf-1 h248
Termination information:
ip/4/vif-0/2 {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = INSERVICE },
        STREAM = 1 {
          LOCALCONTROL { MODE = SENDRECEIVE,
                         DS/DSCP = 00,
                         TMAN/MBS = 0,
                         TMAN/PDR = 0,
                         TMAN/POL = OFF,
                         TMAN/SDR = 0,
                         MGCINFO/DB = 00,
                         GM/RSB = ON,
                         GM/SAF = OFF,
                         GM/SPF = OFF,
                         GM/SPR = 0,
                         GM/ESAS = OFF,
                         GM/ESPS = OFF,
                         GM/LSP = 0 },
          LOCAL {
v=0
c=IN IP4 10.10.0.5
m=- 1024 RTP/AVP -
b=AS:0
          },
          REMOTE {
v=0
c=IN IP4 10.0.0.1
m=- 20002 RTP/AVP -
b=AS:0
          }
        }
      },
      EVENTS = 1001 { NT/QUALERT { TH = 99, STREAM = 1 } },
      SIGNALS
    }

ip/4/vif-0/3 {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = INSERVICE },
        STREAM = 1 {
          LOCALCONTROL { MODE = SENDRECEIVE,
                         DS/DSCP = 00,
                         TMAN/MBS = 1500,
                         TMAN/PDR = 0,
```

```
                              TMAN/POL = OFF,
                              TMAN/SDR = 125000,
                              MGCINFO/DB = 00,
                              GM/RSB = ON,
                              GM/SAF = ON,
                              GM/SAM = "[20.0.0.1]",
                              GM/SPF = OFF,
                              GM/SPR = 0,
                              GM/ESAS = OFF,
                              GM/ESPS = OFF,
                              GM/LSP = 0 },
          LOCAL {
v=0
c=IN IP4 11.0.0.5
m=- 1024 RTP/AVP -
b=AS:0
          },
          REMOTE {
v=0
c=IN IP4 4.0.0.1
m=- 10002 RTP/AVP -
b=AS:0
          }
        }
      },
      SIGNALS
    }
{master}
```

Meaning The show services pgcp terminations gateway *bgf-name* h248 command presents the H.248 parameters as they have been set through H.248 requests and commands from the gateway controller. Comparing this output with the expected H.248 requests reveals whether there was a problem with the requests and commands that the gateway controller sent to the virtual BGF.

Troubleshooting

To troubleshoot the voice configuration:

- No Audio is Reported on a Stream on page 179

No Audio is Reported on a Stream

Problem A call completes correctly (signaling is completed), but the media (audio) stream expected to flow through the BGF fails.

Solution Locate the failed terminations and gates.

1. Acquire the relevant gate IDs termination IDs using the show services pgcp gates command.
2. Display the H.248 parameters for the termination.

```
user@sp-bgf-router> show services pgcp terminations gateway bgf-1
termination-prefix h248 ip/4/vif-0/2
```

```
Termination information:
ip/4/vif-0/2 {
      MEDIA {
        TERMINATIONSTATE { SERVICESTATES = INSERVICE },
        STREAM = 1 {
          LOCALCONTROL { MODE = SENDRECEIVE,
                         DS/DSCP = 00,
                         TMAN/MBS = 0,
                         TMAN/PDR = 0,
                         TMAN/POL = OFF,
                         TMAN/SDR = 0,
                         MGCINFO/DB = 00,
                         GM/RSB = ON,
                         GM/SAF = OFF,
                         GM/SPF = OFF,
                         GM/SPR = 0,
                         GM/ESAS = OFF,
                         GM/ESPS = OFF,
                         GM/LSP = 0 },
          LOCAL {
v=0
c=IN IP4 3.99.99.100
m=- 1024 RTP/AVP -
b=AS:0
          },
          REMOTE {
v=0
c=IN IP4 3.0.0.1
m=- 20002 RTP/AVP -
b=AS:0
          }
        }
      },
      EVENTS = 1001 { NT/QUALERT { TH = 99, STREAM = 1 } },
      SIGNALS
    }
```

3. Display information about the gate.

```
user@sp-bgf-router> show services pgcp gate gateway gate-id 4295033088

Gate information:
Gate id: 4295033088
Gate state:  active
Action: forward
Service set id: 1
Media card: sp-1/2/0
Media handler: bgf1-svc-set
Termination-id-string: ip/4/vif-0/2
```

Using the preceding information, review and verify the following:

1. Terminations are in the In-Service state.

If the termination is in the Out-of-Service state, no streams are allowed access to the termination. The Out-of-Service state indicates a problem with either the resources on the BGF or incorrect parameters requested by the gateway controller.

2. The termination H.248 parameters are as expected.

   Pay special attention to the LOCAL and REMOTE parameters, and make sure they are aligned with the Session Description Protocol (SDP) offered by both elements participating in the session. Also, missing or unknown values suggest a problem with the call setup initiated by the gateway controller.

3. Gate actions are in the Forward state.

   If one or all gates are in the Drop state, no stream is allowed to flow through it, so one-way or no audio results. If a gate is not in the Forward state, the gateway controller might have failed to provide a required descriptor.

   Gate actions in the Forward state, but no media is flowing (frame count is zero or not advancing), can be caused by one of the following problems:

   - Networking or routing issues, including:
     - Stream fails to reach the router. A problem exists with the network path between the stream originator and the BGF gates.
     - Routing Engine, PIC, or DPC failure. The stream reaches the router, but the PIC or DPC fails to receive the stream. Use the show services pgcp active-configuration command to review the PIC or DPC status, and make sure that it is In-Service.
   - Hardware or element failure. The originator fails to send the stream. Use the debug tools available on the VoIP element to verify that the streams have left the element.
   - The originator is using a different source IP address than the one reported in the H.248 termination. Verify that the H.248 termination information matches the stream source and destination received by the BGF and the PIC or DPC. You can use the capture feature on the router to verify that the streams are received on the Packet Forwarding Engine.

Related Topics

- Overview of the BGF VoIP Solution on page 39
- Configuring the BGF on page 63
- For a description of PGCP statements, see *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- For a description of the fields in show commands, see *Chapter 27, PGCP Operational Mode Commands for the BGF Feature* in *JUNOS System Basics and Services Command Reference*

Part 3
IMSG VoIP Solution

Chapter 11

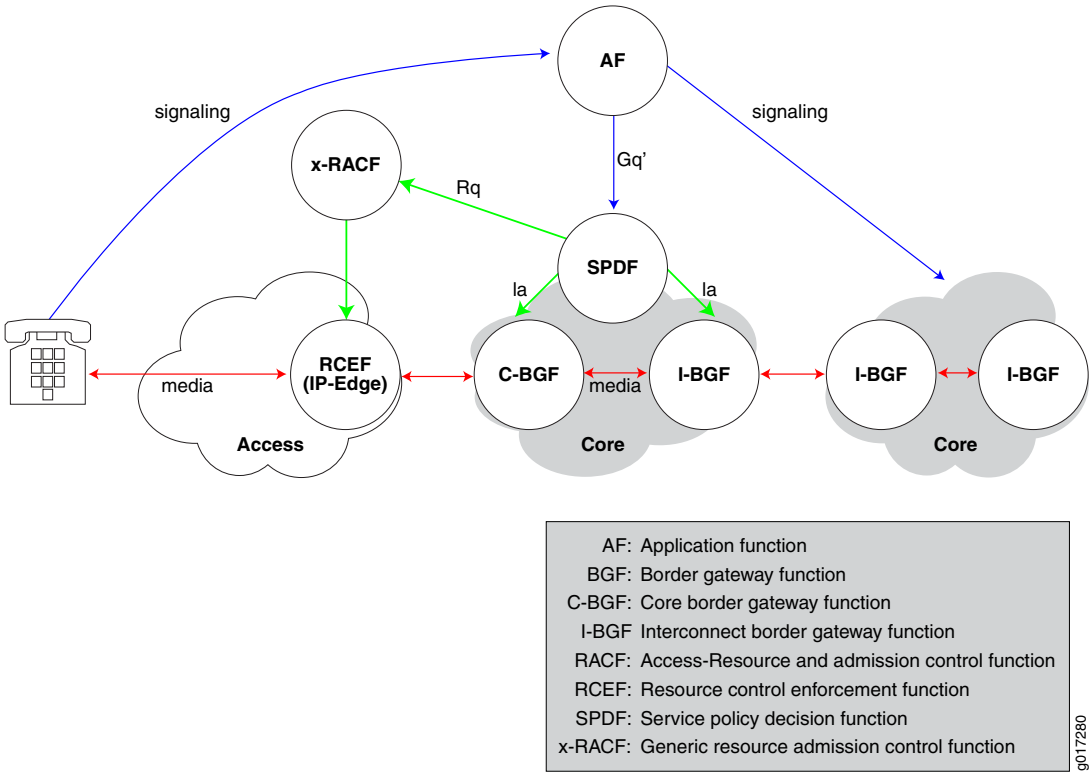
Overview of the IMSG

This chapter describes the Integrated Multi-Service Gateway (IMSG). Topics include:

IMSG VoIP Solution Overview

The IMSG provides the session border controller (SBC) role in the European Telecommunications Standards Institute (ETSI) Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN) architecture as shown in Figure 26 on page 186. The SBC functionality encompasses the AF, SPDF, and BGF components.

Figure 26: IMSG in the ETSI-TISPAN Architecture



IMSG Terms and Abbreviations

Table 14 on page 186 defines the terms and abbreviations used in this topic.

Table 14: Terms and Abbreviations

Term	Description
B2BUA	Back-to-back user agent. A B2BUA is a SIP user agent to both ends of a SIP call. That is, it both establishes and terminates a call. In the TISPAN model, the B2BUA provides the application functions (AF). In the IMSG, the BSG acts as a B2BUA.
BGF	Border gateway function. Resides in the transport layer and polices and enforces traffic flows based on instructions from the SPDF.
BSG	Border signalling gateway. The BSG controls VoIP media resources on the router and is responsible for all SIP processing. The border signalling gateway provides a full B2BUA implementation and an embedded SPDF.
Dialog	A peer-to-peer SIP relationship between two user agents that persists for some time.
Gq'	Interface between the AF (in the IMSG, this is the B2BUA) and the SPDF that is used to exchange session-based policy setup information between the SPDF and the AF.

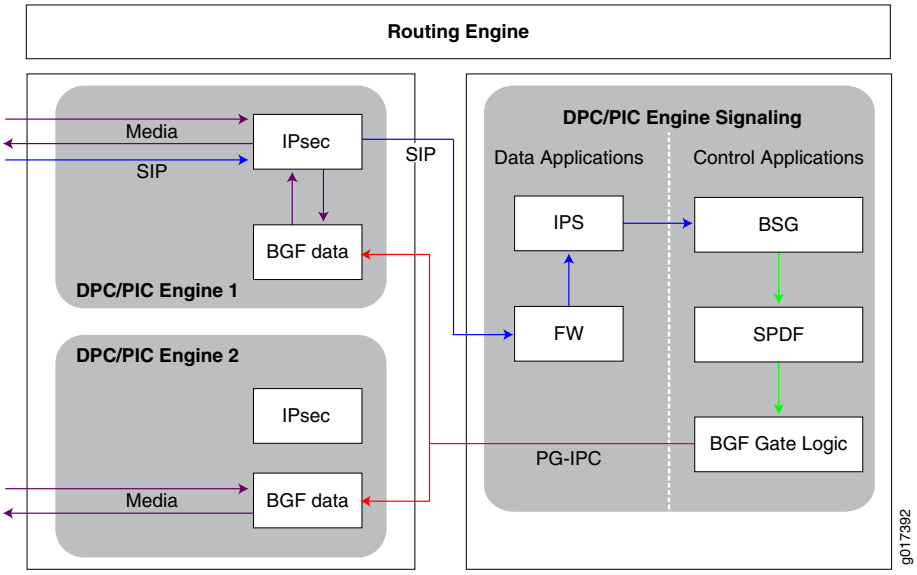
Table 14: Terms and Abbreviations *(continued)*

Term	Description
Ia	A profile of the interface between an SPDF and the BGF.
SIP	Session Initiation Protocol.
SPDF	Service policy decision function. The BSG contains an embedded SPDF that controls the instructions that the BSG sends to the BGF.

IMSG Architecture

Figure 27 on page 187 shows the main components of the IMSG architecture.

Figure 27: IMSG Architecture



BGF

In the IMSG architecture, the BGF controls VoIP signaling and media based on instructions that it receives from the Service Policy Decision Function (SPDF). The BGF process runs on a data PIC.

BSG

The BSG (Border Signaling Gateway) is the component that controls VoIP media resources on the router and is responsible for all SIP processing.

The BSG acts as a Session Initiation Protocol (SIP) back-to-back user agent (B2BUA) that fully terminates incoming signaling sessions and then starts a new signaling session on its other side.

SPDF

Each BSG instance has an embedded SPDF that is a standard TISPAN component with Gq' and Ia interfaces as defined by TISPAN. (See Figure 26 on page 186.)

The SPDF is responsible for:

- Implementing media resource allocation
- Authorizing media resource requests
- Load balancing between BGFs
- Mapping of media type and service class for:
  - DSCP marking
  - Quality of service

How the SPDF Works

The SPDF configuration uses service classes that classify media sessions and then specify the actions to take on the media session—marking, dropping, or applying QoS parameters.

The SPDF coordinates resource reservation requests that it receives from the application function (in this case the B2BUA in the BSG) as follows:

1. The B2BUA sends to the SPDF a summary of any new media session that is signaled through SIP (for example, a gold-class, 256 Kbps, audio/video call is about to start between IP1 and IP2).
2. The SPDF determines whether the request received from the BSG is consistent with the policies defined in the SPDF.
3. If the request is consistent with defined policies, the SPDF maps the session information into:
   - The BGF to be used.
   - The gates and gate parameters to be installed on the BGF.

IPS and FW Applications

You can use the JUNOS Software intrusion prevention system (IPS) technology and stateful firewall features on the same service PIC or DPC as the BSG to provide security services to SIP signaling traffic before the traffic reaches the BSG. This feature uses a simple provisioning model where all of the BSG protection elements are collected in a service set that is applied on a service interface. After the service set processes the traffic, the traffic is sent to the BSG.

IPsec

IPsec is an optional software feature supported by the MultiServices PIC and MS-DPC. The IPsec feature supports Data Encryption Standard (DES), triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). The IMSG can use IPsec to establish mutual authentication between the signaling agents and to negotiate keys used during the session to protect flows and assets.

BSG Policy Overview

The BSG uses policies to control system behavior and to determine how VoIP signaling is handled on a services PIC or MS-DPC. All incoming VoIP requests are matched against policies, and the actions defined in the matching policies determine how the request is handled; for example, which INVITE requests to accept and which to reject. Each BSG feature, such as QoS, call admission control, and routing of SIP requests, is controlled by policies and has its own actions.

There are two types of policies:

- New transaction policies—Define how the BSG handles signaling for new dialogs and for out-of-dialog transactions. A new transaction event is raised when a new SIP request, such as an INVITE, either opens a new dialog or is not related to any dialog. If the event does not match a new transaction policy, the BSG rejects the SIP request and returns a 403 (Forbidden) message.

  The actions that you can take on requests that match conditions in new transaction policies include accepting, rejecting, or tracing traffic; routing of SIP requests; applying CAC (call admission control); adding, modifying, or removing fields in SIP headers; modifying the request URI in SIP messages; or rejecting SIP messages based on information in the SIP header.

- New call policies—Define how the BSG handles media sessions (voice and video). New call policies classify media and provision the actions to take on media streams, such as mark, drop, applying QoS, applying media anchoring, or detecting latch deadlocks or other media inactivity on a gate.

BSG Policy Model

BSG policies are made up of terms that contain conditions and actions that cause the BSG to handle incoming requests in a certain way.

- Condition—The from statement in the policy. Defines values or fields that a request must contain before an action is triggered; for example, a source address, contents of the contact or request URI fields, a SIP method, or a media type, such as audio or video.
  - If you have multiple matching fields defined in a from clause within the same term, an AND function is between the conditions. For example, if you have both a contact defined and a SIP method defined, the term must match the values defined for both the contact and the SIP method.

- If you have multiple definitions for the same field in a from clause, an OR function is between the values in the condition. For example, if you have multiple values defined for a contact, the term must match one the values defined.

- Action—The then statement in the policy. Specifies the action that is performed on incoming traffic that matches the condition; for example, accept or reject, mark with a DSCP code point, apply QoS, or route to a next-hop or egress point.

If you have a policy that includes multiple terms, the software applies the actions in the first term that matches the policy.

Policy Sets

You can configure policy sets, which are a list of policies that you can then apply to a service point. All policies in a set are evaluated. The order in which you add policies to the set determines the order in which the BSG processes the policies. In each policy, the action in the first term that matches is the action that is applied.

Service Points

Service points identify a service interface and transport parameters for incoming requests. You attach policies to the service point, and all requests that arrive at the service point are handled by these policies. You can also configure a service point to be used as an egress service point to which SIP requests are routed. Each BSG can have five service points.

A service interface that you use for service points is a service interface that has been configured for the BSG. See “Configuring the Services PIC or DPC for the BSG” on page 199.

You can configure a VPN on the service point so when you set the egress service point, the packet is sent on a VPN.

Manipulation of Headers and Request URIs in SIP Messages

The header manipulation feature enables you to add, modify, or remove fields in SIP headers and to modify the request URI in SIP messages. It also enables you to reject SIP messages based on information in the SIP header.

This feature is useful for solving interoperability issues between vendors and peers.

How Header Manipulation Works

To use this feature, you set up message manipulation rules and then add the rules to new transaction policies. Message manipulation rules can specify the following actions for SIP headers:

- add—Add an instance of the header field.
- add-missing—Add a new header field if the header field is missing from the SIP header.

- add-overwrite—Add a new header field if the header field is missing from the SIP header. If the header field already exists, its field value is overwritten with the new field value that you specify.
- modify-regular-expression—Change the value of a regular expression.
- remove-all—Remove all instances of the header field.
- remove-regular-expression—Remove all of the header fields that have field values that match the regular expression that you specify.
- reject-regular-expression—Reject SIP messages and terminate the usage that the message is part of.

You can also set up message manipulation rules that specify the modifications that you want to perform on regular expressions in the request URI of SIP messages.

Applying Message Manipulation Rules

After you create your message manipulation rules, you apply them using new transaction policies. Message manipulation affects the transaction that matches the policy as well as any transactions that belong to a dialog that results from the transaction.

You can apply the message manipulation rules in the following directions:

- Forward—Applied to any message going from the user agent client (UAC), or the caller, to the user agent server (UAS), or the call recipient.
- Reverse—Applied to any message going from the UAS (the call recipient) to the UAC (the caller).

Header Manipulation Examples

This topic provides examples of manipulating SIP headers.

Example: Removing a Text String from the Alert-Info Field

Action Apply the remove-alert-info manipulation rule to the forward direction in a new transaction policy:

```
manipulation-rule remove-alert-info {
    actions {
        sip-header Alert-Info {
            field-value {
                remove-regular-expression DummyDomain;
            }
        }
    }
}
```

Result The second appearance of Alert-Info in the following example is removed:

```
Alert-Info:<http://www.example.com/sounds/moo.wav>
Alert-Info:<http://www.DummyDomain.net/user/ringback.mp3>
Alert-Info:<http://wwww.example.com/alice/photo.jpg>
```

Example: Rejecting a Message Based on the Field Value of the From Header

Action Apply the reject-from manipulation rule to the forward direction in a new transaction policy:

```
manipulation-rule reject-from {
    actions {
        sip-header From {
            field-value {
                reject-regular-expression anonymous;
            }
        }
    }
}
```

Result A received SIP message request with From header with the following field value is rejected with a 403 Forbidden SIP response.

From: Anonymous <sip:anonymous@atlanta.com>;tag=1928301774

Example: Using a Regular Expression to Modify the P-Asserted-Identity Field Value

Action Apply the modify-p-asserted-identity manipulation rule to the forward direction in a new transaction policy:

```
manipulation-rule modify-p-asserted-identity {
    actions {
        sip-header P-Asserted-Identity {
            field-value {
                modify-regular-expression "sip:[0-9]+@.*" with
"sip:P-Asserted-Identiy@juniper.net";
            }
        }
    }
}
```

Result A ReINVITE request received from the UAS with P-Asserted-Identity: sip:987654321@SomeDomain.com, is modified to P-Asserted-Identity: sip:P-Asserted-Identiy@juniper.net and then forwarded toward the UAC.

Example: Adding the Transport Protocol and "q" Parameter to the Contact Header

Action Apply the add-transport-q manipulation rule to the forward direction in a new transaction policy:

```
manipulation-rule add-transport-q {
    actions {
        sip-header contact {
            field-value {
               modify-regular-expression "(.*)" with "<\1;transport=UDP>;q=0.7";

            }
```

```
        }
    }
}
```

Result A request received from with Contact: sip:70.100.101.1, is modified to Contact: <sip:70.100.101.1:5060;transport=UDP>;q=0.7.

Using High Availability with Message Manipulation

In the case of an active standby switchover, dialogs that were matched to a policy before the switchover continue to use the policy even if the policy is modified or deleted from the CLI.

In the case of a stateful restart, the new BSG process applies message manipulation rules to dialogs that were already matched to a policy before the switchover occurred as follows:

- If the policy did not change, the same rule is applied to new messages on the dialog.
- If the message manipulation rule was modified, the new rule is applied to new messages on the dialog.
- If the message manipulation rule was deleted, no header manipulation is applied to new messages on the dialog.

Displaying Message Manipulation Rules That Are Currently Being Applied

You can use the following show commands to view the message manipulation rules that are currently being applied to active calls on a specific BSG:

show services border-signaling-gateway by-contact *contact* detailed gateway *gateway-name*
show services border-signaling-gateway by-request-uri *request-uri* detailed gateway *gateway-name*

Media Anchoring Overview

Media anchoring is the act of processing Session Description Protocol (SDP) transactions. SDP transactions are requests for media resources. These requests must be supervised, and allocation must take into account business, security, and performance requirements.

The basic requirements of media anchoring are:

- Hiding the topology of the media network by using NAT.
- Applying bandwidth restrictions and setting the DSCP on processed media packets

The SPDF is the component that applies media anchoring. In new call usage policies you specify whether or not media anchoring is applied.

SIP Routing Overview

The BSG uses SIP routing to determine the next-hop and exit point of SIP messages. You define SIP routing in policies. Each incoming SIP request is matched to a policy that specifies how the SIP request is routed.

You can configure the policy to match incoming SIP requests to:

- Contact field in the SIP message
- Request URI field in the SIP message
- Type of SIP method
- Source addresses and masks

You can specify the following actions to be taken on SIP requests that match the policy:

- Next hop—You can specify the next-hop as a request URI or as a static IP address.
- Egress service point—You can specify the IP address of the interface from which SIP requests exit the router and set a port number and transport protocol used to route the request.

Related Topics

- Using New Transaction Policies to Route SIP Requests on page 209

Virtual Interfaces and NAT Pool Assignment with the IMSG

When a BSG serves as gateway controller for a virtual BGF, the BGF and the controller communicate through virtual interfaces that are associated with media resources. You configure virtual interfaces on the BGF and these virtual interfaces are available to the BSG. The virtual interfaces define media services and their associated NAT pools. You control which media resources the BGF uses by including *default media realm* in service point configurations. The default media realm is a number that matches the number of a defined virtual interface. The BGF uses the NAT pool associated with the virtual interface for traffic passing through the service-point.

IMSG VPN Routing Overview

VPN aggregation using the IMSG works as described in “VPN Aggregation for VoIP Calls Overview” on page 57. However, in the IMSG solution, the BSG provides the B2BUA (gateway controller) functionality, and must be configured to direct VPN traffic to properly configured service interfaces.

To support VPNs, the BSG must be able to:

- Send messages to a specific IP address, port, and VPN.
- Distinguish on which IP address, port, and VPN a particular message arrived.
- For connected transports, such as TCP, the equivalent requirement applies to each connection.

When using the BSG, you specify a VPN by relating a service-interface (interface + unit) to a service-point. The service interface defines the VPN for both incoming and outgoing messages. A separate listening socket is opened for each tuple of: service-interface, address, port, and transport-protocol. The service-interface parameter of the service-point now serves as the VPN identifier. If no unit is specified for the service-interface, unit 0 is implicitly assigned. If no egress service point is specified, the ingress service point is used for the outgoing messages, hence over the same VPN.

Related Topics

- Configuring Routing of VPN Calls on page 216

SIP Timers Overview

The BSG uses SIP timers to clean up calls that are initiated but never established and established calls that are inactive.

SIP Timers for Calls in Initiation Stage

For calls in the initiation stage, the BSG uses Timer C as defined in *RFC 3261 SIP: Session Initiation Protocol*. For every INVITE request sent, an expiration time is calculated as the minimum time between the incoming INVITE request's Expire header and the value configured for Timer C. Timer C works as follows:

- When the INVITE request is sent, an expiration timer is set.
- When a non-100 provisional request arrives, the timer is reset to its original value.
- When a final response to the INVITE request arrives, the timer is canceled.

If the final response to the invite request is not received by the time Timer C expires, the invite is cancelled by sending a CANCEL message to the call recipient and a 408 error message (Request timeout) is sent to the caller.

SIP Timers for Established Calls

For calls that are already established, an inactivity timer works as follows:

- When the call is established, an inactivity timer is set on the INVITE usage.
- Each new SIP request on that dialog resets the timer to its original value.

If the call is inactive (no signaling on the dialog) for the length of the inactivity time, a BYE message is sent for both user agents on the call.

Related Topics

- Configuring SIP Timers on page 223

Providing QoS for VoIP Traffic Overview

The SPDF supports quality of service (QoS) functionality that you can apply for different levels of quality to different types of media. For example, you can configure

one set of QoS parameters for a video stream and a different set of parameters for a voice stream. With this feature, you can divide your network into segments and allocate resources to those segments according to your company's business model. For example, customers who pay more can get more bandwidth or faster bandwidth.

To prevent filling a link to capacity or overfilling a link, which can result in network congestion and poor performance, you can limit media streams to specific bandwidth by specifying a committed information rate and a committed burst size.

Also, you can use DSCP marking to indicate the recommended priority of a media stream to the routers and switches that the media is heading towards.

The SPDF uses service classes to determine system resources. The selection of a service class for a specific stream is based on SIP signaling parameters. A service class has one or more terms that determine whether media of a specific type is allowed, and if it is, the bandwidth restrictions that must be set on packets, as well as their priority. After you create your service classes, you apply them using new call usage policies.

Related Topics
- Configuring QoS on page 223

Providing Call Admission Control (CAC) Overview

With the CAC feature you can prevent voice traffic congestion and ensure that there is enough bandwidth for authorized media sessions by limiting the calls on a connection or link. The BSG applies CAC during call setup to limit the initiation of dialogs and transactions. Dialogs are call attempts or INVITE messages. Transactions are out-of-dialog request messages including REGISTER, OPTIONS, MESSAGE, and INVITE (INVITE messages that open a dialog).

To use CAC, you configure CAC criteria and then apply the criteria using new transaction policy actions. The policy action verifies whether a new event is permitted or not. If it is not permitted, the BSG rejects the dialog or out-of-dialog transaction by sending 403 FORBIDDEN message.

Table 15 on page 196 lists the configurable CAC criteria and their maximum values. These maximum values are used by default.

Table 15: CAC Parameters

CAC Parameter	Maximum (Default) Value
Maximum concurrent dialogs	100,000
Maximum dialog attempts per second	100
Maximum dialog attempts burst size	200
Maximum concurrent transactions	50,000
Maximum transaction attempts per second	1500
Maximum transaction attempts burst size	3000

Chapter 12

Configuring the IMSG

This chapter explains how to configure the IMSG. Topics include:

Enabling the BSG Service Package on the PIC or DPC

The BSG can run on Adaptive Services (AS) and MultiServices PICs or on a MultiServices Dense Port Concentrator (MS-DPC). You must enable the BSG service package on the services PIC or DPC before you can configure the BSG software. The name of the BSG service package is jservices-voice.

Step-by-Step Procedure To enable the BSG service package on a PIC or DPC:

1. Determine the FPC slot number and the PIC number of the services PIC or DPC on which you want to enable the BSG service package.

   In the following example, the FPC slot number is 0 and the PIC number is 3.

```
user@host>show chassis hardware
Hardware inventory:
Item           Version  Part number  Serial number     Description
.
.
.
FPC 0                                E-FPC
  PIC 0        REV 11   750-002971   RH1375            4x OC-3 SONET, MM
  PIC 1        REV 12   750-012838   DN0449            4x 1GE(LAN), IQ2
    Xcvr 0     REV 01   740-013111   8142659           SFP-T
    Xcvr 1     REV 01   740-013111   8142630           SFP-T
    Xcvr 2     REV 01   740-013111   8155199           SFP-T
    Xcvr 3     REV 01   740-013111   8154799           SFP-T
  PIC 2        REV 11   750-005724   RH2051            2x OC-3 ATM-II IQ, MM
  PIC 3        REV 15   750-014895   DN3277            MultiServices 100
.
.
.
```

2. Enable the jservices-voice package on the PIC or DPC.

```
[edit chassis]
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   package jservices-voice
```

3. Set the number of megabytes that can be used for the wired process memory, which is virtual memory used to reduce Translation Look-aside Buffer (TLB) misses.

```
[edit chassis]
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   wired-process-mem-size 512
```

4. Set the number of processing cores dedicated to the control functionality of the jservices-voice application.

```
[edit chassis]
```

```
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
  control-cores 7
```

5. Specify that the PIC or DPC not restart if the routing engine is swapped.

```
[edit chassis]
user@host#set no-service-pic-restart-on-failover
```

6. Commit your configuration changes. You must perform the commit before you can proceed to configure the IMSG.

```
[edit]
user@host#commit
commit complete
```

Setting Up System Processes

When you use the BSG to control the BGF, you need to enable the SBC configuration process for the BSG and disable the pgcpd process for the BGF.

Step-by-Step Procedure To set up system processes.

1. Access the system process configuration.

```
[edit]
user@host#edit system processes
```

2. Enable the SBC configuration process for the BSG.

```
[edit system processes]
user@host#activate sbc-configuration-process
```

3. Disable the pgcpd process for the BGF.

```
[edit]
user@host#set pgcp-service disable
```

Configuring the Services PIC or DPC for the BSG

You need to configure an AS or MultiServices PIC or MS-DPC for the BSG.

Step-by-Step Procedure To configure the PIC or MS-DPC:

1. Enter edit mode for the PIC or DPC.

```
[edit]
user@host#edit interfaces ms-0/3/0
```

2. Configure a logical unit and enter edit mode for the logical unit.

```
[edit interfaces ms-0/3/0]
user@host#edit unit 0
```

3. Specify the protocol family and configure an address for the BSG.

```
[edit interfaces ms-0/3/0 unit 0]
user@host#set family inet address 10.10.200.20/32
```

4. Configure a description.

```
[edit interfaces ms-0/3/0 unit 0]
user@host#set description BSG-Service-PIC
```

Configuring the Services PIC or DPC for the BGF

You need to configure an AS or MultiServices PIC or MS-DPC for the BGF.

Step-by-Step Procedure To configure the PIC or MS-DPC:

1. Enter edit mode for the interface.

```
[edit]
user@host#edit interfaces sp-0/2/0
```

2. Configure a description for the interface.

```
[edit interfaces sp-0/2/0]
user@host#set description BGF-Service-PIC
```

3. Configure logical unit 0, and specify the protocol family and the address of a virtual BGF.

```
[edit interfaces sp-0/2/0]
user@host#set unit 0 family inet address 10.10.200.21/32
```

4. Configure a logical unit and specify the protocol family.

```
[edit interfaces sp-0/2/0]
user@host#set unit 10 family inet
```

5. Set the service domain of the logical unit to inside. This unit number must match the unit number of the inside service interface configured in the service set.

```
[edit interfaces sp-0/2/0]
user@host#set unit 10 service-domain inside
```

6. Configure a logical unit and specify the protocol family.

```
[edit interfaces sp-0/2/0]
user@host#set unit 20 family inet
```

7. Set the service domain of the logical unit to outside. This unit number must match the unit number of the outside service interface configured in the service set.

```
[edit interfaces sp-0/2/0]
user@host#set unit 20 service-domain outside
```

8. Configure system logging on the service interface.

```
[edit interfaces sp-0/2/0]
user@host#set services-options syslog host local services any
```

Related Topics

- *Chapter 24, Interface Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 25, Summary of Interface Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring NAT Pools

Step-by-Step Procedure To configure a NAT pool:

1. Create a NAT pool, and specify a name for the pool.

   ```
   [edit services]
   user@host#edit nat pool bsg_rtp_nat_pool
   ```

2. Configure an address range for the pool.

   ```
   [edit services nat pool bsg_rtp_nat_pool]
   user@host#set address-range low 10.10.20.100 high 10.10.30.100
   ```

3. Configure a range of ports, or specify that ports are automatically assigned.

   ```
   [edit services nat pool bsg_rtp_nat_pool]
   user@host#set port automatic
   ```

4. Specify that the NAT pool is used exclusively by the BGF.

   ```
   [edit services nat pool bsg_rtp_nat_pool]
   user@host#set pgcp
   ```

5. Configure the number of ports allocated to voice and video flows on each gate. By default two ports are available. However, if you want to allocate two ports—one for video and one for voice—to both the Real-Time Transport Protocol (RTP) and the accompanying Real-Time Control Protocol (RTCP) flow, specify four ports.

   ```
   [edit services nat pool bsg_rtp_nat_pool]
   user@host#set pgcp ports-per-session 2
   ```

Related Topics

- *Chapter 9, Summary of Network Address Translation Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*
- Twice NAT for VoIP Traffic Overview on page 49

Assigning a NAT Pool

To assign a NAT pool, you create a media service configuration that contains the name of the NAT pool. You then specify the media service in a virtual interface

configuration and in a PGCP rule. The PGCP rule assigns the media service for a specific virtual BGF.

Step-by-Step Procedure To configure a media service:

1. Create a media service, and specify a name for the service.

```
[edit services pgcp]
user@host#edit media-service media-service-one
```

2. Assign the NAT pool to the media service.

```
[edit services pgcp media-service media-service-one]
user@host#set nat-pool bsg_rtp_nat_pool
```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Virtual Interfaces

The virtual interface configuration determines the NAT pool (media service) for calls to use.

Step-by-Step Procedure To configure a virtual interface:

1. Create a virtual interface, and assign the number 0 to the interface.

```
[edit services pgcp]
user@host#edit virtual-interface 0
```

2. Specify the name of the media service that contains the NAT pool to be used for gates on the virtual interface that you are configuring.

```
[edit services pgcp virtual-interface 0]
user@host#set media-service media-service-one
```

3. Set the virtual interface to in service.

```
[edit services pgcp virtual-interface 0]
user@host#set service-state in-service
```

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Creating a Rule That Specifies the NAT Pool to Use on a Virtual BGF

Rules for the BGF are applied on the services PIC or DPC. The rules combined with firewall rules specify to the PIC or DPC how to deal with media traffic. The BGF rules specify the NAT pool (media service) used on a specific virtual BGF.

Step-by-Step Procedure To configure a rule:

1. Create a rule and specify a name for the rule.

   ```
   [edit services pgcp]
   user@host#edit rule bgf-rule-1
   ```

2. Specify the virtual BGF on which this rule is applied.

   ```
   [edit services pgcp rule bgf-rule-1]
   user@host#set gateway bgf-1
   ```

3. Specify the media service that contains the NAT pool to be used for this virtual BGF.

   ```
   [edit services pgcp rule bgf-rule-1]
   user@host#set media-service media-service-one
   ```

You can also configure rules for the BGF within a service set.

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Specifying the Order in Which the BGF Processes Rules

If you define multiple rules, you can specify the order in which the BGF processes the rules by creating a rule set. The BGF processes the rules in the order in which you specify them in the rule set. It processes rules as follows:

- If a rule matches the packet, the BGF performs the corresponding action and the rule processing stops.
- If no rule matches the packet, processing continues to the next rule in the set. If none of the rules match the packet, the packet is dropped by default.

Step-by-Step Procedure

To configure a rule set.

1. Create a rule set and specify a name for the rule set.

   ```
   [edit services pgcp]
   user@host#edit rule-set bgf-rule-set-1
   ```

2. Add a rule to the rule set.

   ```
   [edit services pgcp rule-set bgf-rule-set-1]
   user@host#set rule bgf-rule-1
   ```

3. Add additional rules to the rule set.

   ```
   [edit services pgcp rule-set bgf-rule-set-1]
   user@host#set rule bgf-rule-2
   ```

You can also configure rule sets for the BGF within a service set.

Related Topics
- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Stateful Firewall

Step-by-Step Procedure To create a stateful firewall:

1. Create a stateful firewall rule.

```
[edit services stateful-firewall]
user@host#edit rule r1
```

2. Set the match direction for the rule.

```
[edit services stateful-firewall rule r1]
user@host#set match-direction input-output
```

3. Add a term to the rule.

```
[edit services stateful-firewall rule r1]
user@host#set term t1 then reject
```

Related Topics
- *Chapter 7, Summary of Stateful Firewall Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Service Set

A service set lets you combine rules for different services into one set and then apply the set of services to inside and outside interfaces on a MultiServices PIC or MS-DPC. You need to configure a service set for each PIC or DPC.

In this case, we are creating a service set that does the following:

- Combines the stateful firewall and BGF rules to be used on the PIC. The BGF rule is the rule that associates the virtual BGF with a NAT pool.
- Applies the combined rules to an inside and outside interface on the MultiServices PIC or MS-DPC that was created for the BGF service.
- Defines a location and logging level for the service set.

Step-by-Step Procedure To configure a service set:

1. Create a service set configuration.

```
[edit services]
user@host#edit service-set bgf-svc-set
```

2. Specify the name of the BGF rule or rule set that applies to this service set.

```
[edit services service-set bgf-svc-set]
user@host#set pgcp-rules bgf-rule-1
```

3. Specify the name of the stateful firewall rule that applies to this service set.

```
[edit services service-set bgf-svc-set]
user@host#set stateful-firewall-rules r1
```

4. Configure service set as a next-hop service set.

```
[edit services service-set bgf-svc-set]
user@host#edit next-hop-service
```

5. Specify the service interface to the inside network. This is the logical interface that you configured as the inside service domain on the MultiServices PIC or MS-DPC that you configured for the BGF.

```
[edit services service-set bgf-svc-set next-hop-service]
user@host#set inside-service-interface sp-0/2/0.10
```

6. Specify the service interface to the outside network. This is the logical interface that you configured as the outside service domain on the MultiServices PIC or MS-DPC that you configured for the BGF.

```
[edit services service-set bgf-svc-set next-hop-service]
user@host#set outside-service-interface sp-0/2/0.20
```

7. Configure a location and logging level for the service set.

```
[edit services service-set bgf-svc-set]
user@host#edit syslog host local-1
[edit services service-set bgf-svc-set syslog host local-1]
user@host#set services any
```

Related Topics

- *Chapter 22, Service Set Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 23, Summary of Service Set Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Virtual BGF

Step-by-Step Procedure

To configure a virtual BGF:

1. Create a virtual BGF, and assign a name to the virtual BGF. You can configure an IP address as the virtual BGF name. However, the IP address is not used in the operation of the virtual BGF.

```
[edit services pgcp]
user@host#edit gateway bgf-1
```

2. Specify the IP address of the virtual BGF. This address is the address of the services PIC or DPC that you configured for the BGF.

```
[edit services pgcp gateway bgf-1]
user@host#set gateway-address 10.10.200.21
```

3. Specify the port number of the virtual BGF.

```
[edit services pgcp gateway bgf-1]
user@host#set gateway-port 2944
```

4. Specify the services PIC or DPC on which the BGF process runs.

```
[edit services pgcp gateway bgf-1]
user@host#set platform device ms-0/3/0
```

5. Set the virtual BGF to in service.

```
[edit services pgcp gateway bgf-1]
user@host#set service-state in-service
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Creating BSG Instances

You can create one BSG instance. The BSG instance needs to be associated with a services PIC or DPC.

Step-by-Step Procedure

To configure a BSG instance:

1. Create a BSG, and assign it a name.

```
[edit services]
user@host#edit services border-signaling-gateway gateway bsg-1
```

2. Specify the services PIC or DPC that you configured for the BSG.

```
[edit services border-signaling-gateway gateway bsg-1]
user@host#set service-interface ms-0/3/0
```

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a Gateway Controller

Step-by-Step Procedure

To configure a gateway controller:

1. Create a gateway controller configuration, and assign a name to the gateway controller.

```
[edit services pgcp gateway bgf-1]
user@host#edit gateway-controller bsg-1
```

2. Specify the BSG to control the virtual BGF.

```
[edit services pgcp gateway bgf-1 gateway-controller bsg-1]
user@host#set local-controller bsg-1
```

3. Specify the IP address of the gateway controller. This is the address of the services PIC or DPC that you configured for the BSG.

```
[edit services pgcp gateway bgf-1 gateway-controller bsg-1]
user@host#set controller-address 10.10.200.20
```

4. Configure the number of the gateway controller listening port.

```
[edit services pgcp gateway bgf-1 gateway-controller bsg-1]
user@host#set controller-port 2944
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Using Regular Expressions to Match Incoming SIP Messages to Policies

You can use regular expressions to match the information in the contact and request URI fields of incoming SIP messages. You configure the regular expressions in the from condition of new call usage policies and new transaction policies. Table 16 on page 207 describes the regular expressions supported for policies.

If you use parentheses or spaces in your regular expression, you must enclose the expression in double quotation marks.

Table 16: Regular Expressions Supported for Policies

Operator	Matches
.	Any single character including a space
*	0 or more instances of a character or pattern
+	1 or more instances of a character or pattern
?	0 or 1 instances of a character or pattern
( )	Group of expressions.
|	One of the two terms on either side of the pipe
[*start-end*]	Range of characters
[^*start-end*]	One instance of any character that is not in the range
[A-Za-z0-9_]	Any alphanumeric character

Examples of Regular Expressions Used for VoIP Calls

Table 17 on page 208 provides examples of regular expressions used in the request URI or contact fields of policies.

Table 17: Examples of Regular Expressions Used for VoIP Calls

Type of Information to Match	Example of Traffic to Match	Regular Expression Used
Emergency 911 calls	911	"sip:911@.+ | tel:911"
International calls	011xxxxxxxx	"+:011[0-9]+@.+ | tel:011[0-9]+"
Access to outside line	9	"sip:9[0-9]+@.+ | tel:9[0-9]+"
Area code and 1 + dialing	1 408/506	"sip:(1(408|506)([0-9]+)@.+) | (tel:1(408|506)([0-9]+))"
Emergency calls	x11	"sip:[2-9]11@.+ | tel:[2-9]11"
Domain name	@juniper.net	.*@juniper.net

Configuring a New Transaction Policy

New transaction policies control how requests related to new transactions are handled. A new transaction event is raised when a new SIP request message, such as an INVITE, either opens a new dialog or is not related to any dialog. If the event does not match a new transaction policy, the BSG rejects the SIP request and returns a 403 (Forbidden) message.

The actions that you can take on requests that match conditions in new transaction policies include accepting, rejecting, or tracing traffic; routing of SIP requests; or applying CAC (call admission control). Using new transaction policies to route SIP requests or to apply CAC is described separately.

Step-by-Step Procedure To configure a new transaction policy:

1. Create a new transaction policy, and assign it a name.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip]
   user@host#edit new-transaction-policy peer-to-core
   ```

2. Configure a term for the policy.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
     peer-to-core]
   user@host#edit term block_presence
   ```

3. Configure match conditions for the term. For example, to match incoming traffic based on the type of SIP method:

   ```
   [edit services border-signaling-gateway gateway bsg sip new-transaction-policy
     peer-to-core term block_presence]
   user@host#set from method method-register
   user@host#set from method method-subscribe
   user@host#set from method method-publish
   ```

   If you have multiple values for the same field in a from clause, there is an OR function between the values. In this case, the term must match one of the method values defined.

4. Configure actions to be taken on messages that match the term conditions. For example:

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
    peer-to-core term block_presence]
user@host#set then reject
```

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Using New Transaction Policies to Route SIP Requests

You can route SIP requests by specifying a next-hop action. This action selects the SIP entity towards which SIP requests are sent. You can configure the next-hop as a static IP address or an address extracted from the SIP request URI. You can also configure the interface, IP address, and port number from which the request exits the BSG by setting an egress service point.

Step-by-Step Procedure

To configure a new transaction policy to route SIP requests:

1. Access the configuration of a new transaction policy.

```
[edit services border-signaling-gateway gateway bsg-1 sip]
user@host#edit new-transaction-policy emergency-call-route
```

2. Configure a term for the policy.

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
    new-transaction-policy emergency-call-route]
user@host#edit term t1
```

3. Configure match conditions for the policy. For example, to match incoming traffic based on the contents of the request URI:

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
    emergency-call-route term t1]
user@host#set from request-uri regular-expression “sip:911@.+ | tel:911”
```

4. Configure actions to be taken on messages that match the term conditions. For example:

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
    emergency-call-route term t1]
user@host#set then route next-hop address 196.10.3.45 port 5060
```

5. Configure an exit point of SIP requests from the BSG. This is a service point that you configure with the service-point statement.

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
    emergency-call-route term t1]
user@host#set then route egress-service-point sip-udp-5060
```

Related Topics

- SIP Routing Overview on page 194

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Message Manipulation Rules

Message manipulation rules specify how you want the BSG to manipulate the header fields or the request URI in SIP messages.

Before You Begin

Note the following before you configure message manipulation rules:

- Incorrect header manipulation rules applied to headers that are responsible for dialog management, such Call-ID, Via, and Contact, and local and remote tags, might cause all calls to fail.
- Manipulating some SIP header fields can result in malformed SIP messages that might cause unexpected behavior such as call failure.
- Some header fields have special treatment that causes them to act differently when the header is manipulated. For example, the Expire header value is set using timer C, which you can configure in the CLI. Therefore, manipulation of this header field has no effect.
- In some cases, rules do not take effect because some fields, such as Call-ID, can be managed and overridden by the software.
- If you receive unexpected results from your header manipulation rules, begin troubleshooting your rules by checking the regular expressions in your rules.
- You can configure up to 1000 manipulation rules for a BSG.

Step-by-Step Procedure

To configure message manipulation rules:

1. Create a new message manipulation rule, assign it a name, and enter the actions configuration.

```
[edit services border-signaling-gateway gateway bsg-1 sip]
user@host#edit message-manipulation-rules manipulation-rule hm-rule actions
```

2. Create a configuration for a SIP header field.

```
[edit services border-signaling-gateway gateway bgf-1 sip
   message-manipulation-rules manipulation-rule hm-rule actions]
user@host#edit sip-header accept-language
```

3. Add field values that you want to manipulate.

```
[edit services border-signaling-gateway gateway bgf-1 sip
   message-manipulation-rules manipulation-rule hm-rule actions sip-header
   accept-language]
user@host#set field-value remove-regular-expression French
user@host#set field-value add Japanese
```

Using New Transaction Policies to Manipulate SIP Headers or to Reject SIP Messages

You can use new transaction policies to modify information in SIP headers or to reject SIP messages based on information in the SIP header.

Step-by-Step Procedure

To configure a new transaction policy to manipulate SIP headers or to reject SIP messages:

1. Access the configuration of a new transaction policy.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip]
   user@host#edit new-transaction-policy tr_accept
   ```

2. Configure a term for the policy.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
     tr_accept]
   user@host#edit term accept_all
   ```

3. Access the message manipulation configuration.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
     tr_accept term accept_all]
   user@host#edit then message-manipulation
   ```

4. Add forward manipulation rules to the policy. Forward manipulation rules are applied to messages going from the user agent client (UAC), or the caller, to the user agent server (UAS), or the call recipient. It is applied to the original transaction request.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
     tr_accept term accept_all then message-manipulation]
   user@host#set forward-manipulation hm-rule
   user@host#set forward-manipulation mod-to
   ```

5. Add reverse manipulation rules to the policy. Reverse manipulation rules are applied to messages going from the UAS (the call recipient) to the UAC (the caller).

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy
     tr_accept term accept_all then message-manipulation]
   user@host#set reverse-manipulation no-subscribe
   ```

Configuring Call Admission Control (CAC)

CAC prevents bottlenecks by limiting new and active dialogs and transactions. You configure CAC criteria in admission control profiles. You then assign the profiles to actions in new transaction policies.

- Configuring Admission Control Profiles on page 212
- Assigning Admission Control Profiles to New Transaction Policies on page 213

Configuring Admission Control Profiles

You can define up to 100 admission control proiles for a BSG.

To cause the software to block all new dialogs or out-of-dialog transactions and to send 403 (Forbidden) messages, set the relevant committed-attempts-rate to 0 and the maximum-burst-size to 0.

Step-by-Step Procedure To configure an admission control profile for CAC:

1. Create an admission control profile.

   ```
   [edit services border-signaling-gateway gateway bsg-1]
   user@host#edit admission-control acprofile1
   ```

2. Access the dialog configuration for this profile.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1]
   user@host#edit dialogs
   ```

3. Configure the maximum number of concurrent dialogs.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     dialogs]
   user@host#set maximum-concurrent 50000
   ```

4. Configure the maximum number of new dialog attempts per second.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     dialogs]
   user@host#set committed-attempts-rate 50
   ```

5. Configure the maximum burst size (number of dialog attempts).

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     dialogs]
   user@host#set committed-burst-size 100
   ```

6. Access the transaction configuration level for this profile.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     dialogs]
   user@host#up 1
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1]
   user@host#edit transactions
   ```

7. Configure the maximum number of concurrent transactions.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     transactions]
   user@host#set maximum-concurrent 50000
   ```

8. Configure the maximum number of new transaction attempts per second.

   ```
   [edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
     transactions]
   ```

```
user@host#set committed-attempts-rate 50
```

9. Configure the maximum burst size (number of transaction attempts).

```
[edit services border-signaling-gateway gateway bsg-1 admission-control acprofile1
   transactions]
user@host#set committed-burst-size 100
```

Assigning Admission Control Profiles to New Transaction Policies

To assign a controller, you add the name of a controller to the then action in a new transaction policy.

Step-by-Step Procedure To assign a profile to a new transaction policy:

1. Access the configuration of the new transaction policy.

```
[edit]
user@host#edit services border-signaling-gateway gateway bsg–1 sip
   new-transaction-policy policy10 term peer-to-peer then
```

2. Assign an admission control profile to the new transaction policy.

```
[edit services border-signaling-gateway gateway bsg–1 sip new-transaction-policy
   policy10 term peer-to-peer then]
user@host#set admission-control acprofile1
```

Related Topics

- Providing Call Admission Control (CAC) Overview on page 196
- Configuring a New Transaction Policy on page 208
- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring New Transaction Policy Sets

You can group new transaction policies into a set. You can then apply the entire set to a service point.

Step-by-Step Procedure To configure a new transaction policy set:

1. Create a new transaction policy set, and assign it a name.

```
[edit services border-signaling-gateway gateway bsg-1 sip]
user@host#edit new-transaction-policy-set peer-to-core
```

2. Add new transaction policies to the policy set.

```
[edit services border-signaling-gateway gateway bsg-1 sip new-transaction-policy-set
   peer-to-core]
user@host#set policy-name [emergency-call-route peer-2-core]
```

All policies in a set are evaluated. The order in which you add policies to the set determines the order in which the BSG processes the policies. In each policy, the action in the first term that matches is the action that is applied.

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring a New Call Usage Policy

Use new call usage policies to classify media and to provision the actions to take on the media streams. Actions can include marking rate limiting.

We suggest that you assign meaningful names to your policies and terms. In this procedure, we are creating a policy for traffic going from the peer to the core. The policy has two conditions, one for voice traffic and one for video traffic.

Step-by-Step Procedure

To configure a new call usage policy instance:

1. Create a new call usage policy, and assign it a name.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip]
   user@host#edit new-call-usage-policy peer-media-2-core
   ```

2. Configure a term for voice traffic coming from the peer.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
     peer-media-2-core]
   user@host#edit term voice
   ```

3. Configure match conditions for the term. For example, to match any call made to area code 555:

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
     peer-media-2-core term voice]
   user@host#set from request-uri regular-expression sip:555.+
   ```

4. Configure the actions taken on media sessions that match the term condition. For example, set the media policy to a service class.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
     peer-media-2-core term voice]
   user@host#set then media-policy service-class voice-high
   ```

5. Configure a term for video traffic coming from the peer.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
     peer-media-2-core]
   user@host#edit term video
   ```

6. Configure match conditions for the term.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
     peer-media-2-core term video]
   user@host#set from request-uri regular-expression sip:121.+
   ```

7. Configure the actions taken on media sessions that match the term condition.

```
[edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
    peer-media-2-core term video]
user@host#set then media-policy service-class video-high
```

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring New Call Usage Policy Sets

You can group new call usage policies into a set. You can then apply the entire set to a service point.

Step-by-Step Procedure

To configure a new call usage policy set:

1. Create a new call usage policy set, and assign it a name.

```
[edit services border-signaling-gateway gateway bsg-1 sip]
user@host#edit new-call-usage-policy-set video
```

2. Add new call usage policies to the policy set.

```
[edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy-set
    gold-customers]
user@host#set policy-name [allow_g729 Voice_mark_AF33 Video_mark_AF22]
```

All policies in a set are evaluated. The order in which you add policies to the set determines the order in which the BSG processes the policies. In each policy, the action in the first term that matches is the action that is applied.

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Attaching Policies to a Service Point

Service points identify a service interface and transport parameters for incoming requests. You attach policies to the service point, and all requests that arrive at the service point are handled by these policies. You can also configure a service point to be used as an egress service point from which SIP requests are routed. Each BSG can have five service points.

Step-by-Step Procedure

To configure a service point:

1. Create a service point, and assign it a name.

```
[edit services border-signaling-gateway gateway bsg-1]
user@host#edit service-point sip-udp-5060
```

2. Assign a service interface to the service point. This is the logical interface that you configured for the BSG.

```
[edit services border-signaling-gateway gateway bsg-1 service-point sip-udp-5060]
user@host#set service-interface ms-0/3/0.0
```

3. Assign transport parameters, which can include any combination of port number, IP address, and transport protocol. Policies are applied only to incoming requests that match the transport parameters. Make sure that the IP address is the address of the service interface that you configured for the BSG.

```
[edit services border-signaling-gateway gateway bsg-1 service-point sip-udp-5060]
user@host#set transport–details port 5060 ip-address 10.10.200.20 udp
```

4. Assign a VoIP protocol as the service point type. Currently, SIP is the only protocol supported.

```
[edit services border-signaling-gateway gateway bsg-1 service-point sip-udp-5060]
user@host#set service-point-type sip
```

5. Attach new transaction service policies or policy sets to the service point.

```
[edit services border-signaling-gateway gateway bsg-1 service-point sip-udp-5060]
user@host#set service-policies new-transaction-policies peer-to-core
```

6. Attach new call usage policies or policy sets to the service point.

```
[edit services border-signaling-gateway gateway bsg-1 service-point sip-udp-5060]
user@host#set service-policies new-call-policies peer-media-2-core
```

Deleting Service Points

Deletion of service points that are handling active calls is not supported. Before you delete a service point, we recommend that you detach it from its policies and wait for the active calls to close.

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Routing of VPN Calls

To route SIP calls between VPN routing instances, you must include interfaces for the BGF and BSG in the routing instances. Configure a service point for each VPN. Assign a *default media realm* for each service point. The default media realm is used to select a pgcp virtual interface, which determines media service and NAT pool. A VPN-based call, like other SIP calls, is routed between service points based on new transaction policies attached to the ingress service point.

Step-by-Step Procedure

To configure routing of VPN calls:

1. Configure router VPN interfaces.

```
[edit interfaces]
user@host#set fe-2/0/1 vlan-tagging unit 0 vlan-id 702 family inet address
  70.2.101.101/16
```

```
user@host#set fe-2/0/1 vlan-tagging unit 10 vlan-id 703 family inet address
  70.100.101.1/24
user@host#set fe-2/0/2 vlan-tagging unit 0 vlan-id 703 family inet address
  70.3.101.101/16
user@host#set fe-2/0/2 vlan-tagging unit 10 vlan-id 702 family inet address
  70.100.102.1/24
```

2. Configure the service interfaces for the BGF.

```
[edit]
user@host#edit interfaces sp-4/0/0 unit 10
[edit interfaces sp-4/0/0 unit 10 ]
user@host#set family inet
user@host#set description "BGF unit for vpn 1"
user@host#edit interfaces sp-4/0/0 unit 20

[edit]
[edit interfaces sp-4/0/0 unit 20]
user@host#set family inet
user@host#set description "BGF unit for vpn 2"
[edit]
user@host#edit interfaces sp-4/0/0 unit 30
[edit interfaces sp-4/0/0 unit 30]
user@host#set family inet
user@host#set description "BGF unit for vpn 3"
user@host#edit interfaces sp-4/0/0 unit 40

[edit]
user@host#edit interfaces sp-4/0/0 unit 40
[edit interfaces sp-4/0/0 unit 40]
user@host#set family inet
user@host#set description "BGF unit for vpn 4"
```

3. Configure the service interfaces for the BSG.

```
[edit]
user@host#edit interfaces ms-4/2/0 unit 10
[edit interfaces ms-4/2/0 unit 10]
user@host#set family inet
user@host#set description "BSG unit for vpn 1"
user@host#set address 70.101.101.2/32

[edit]
user@host#edit interfaces ms-4/2/0 unit 20
[edit interfaces ms-4/2/0 unit 20]
user@host#set family inet
user@host#set description "BSG unit for vpn 2"
user@host#set address 70.101.102.2/32

[edit]
user@host#edit interfaces ms-4/2/0 unit 30
[edit interfaces ms-4/2/0 unit 30]
user@host#set family inet
user@host#set description "BSG unit for vpn 3"
user@host#set address 70.101.103.2/32
```

```
[edit]
user@host#edit interfaces ms-4/2/0 unit 40
[edit interfaces ms-4/2/0 unit 40 family inet]
user@host#set family inet
user@host#set description "BSG unit for vpn 4"
user@host#set address 70.101.104.2/32
```

4. Configure a policy statement to be used for the vrf-import and vrf-export policies that you plan to configure in the routing instances.

```
[edit]
user@host#edit policy-options policy-statement policy-1
[edit edit policy-options policy-statement policy-1]
user@host#set term term1 then reject
```

5. Configure routing instances for each VRF.

```
[edit]
user@host#edit routing-instances vrf_1
[edit routing-instances vrf_1]
user@host#set instance-type vrf
user@host#set interface fe-2/0/1.0
user@host#set interface sp-4/0/0.10
user@host#set interface ms-4/2/0.10
user@host#set route-distinguisher 1:1
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1

[edit]
user@host#edit routing-instances vrf_2
[edit routing-instances vrf_2]
user@host#set instance-type vrf
user@host#set interface fe-2/0/1.10
user@host#set interface sp-4/0/0.20
user@host#set interface ms-4/2/0.20
user@host#set route-distinguisher 1:2
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1

[edit]
user@host#edit routing-instances vrf_3
[edit routing-instances vrf_3]
user@host#set instance-type vrf
user@host#set interface fe-2/0/2.0
user@host#set interface sp-4/0/0.30
user@host#set interface ms-4/2/0.30
user@host#set route-distinguisher 1:3
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1

[edit]
user@host#edit routing-instances vrf_4
[edit routing-instances vrf_4]
user@host#set instance-type vrf
user@host#set interface fe-2/0/2.10
user@host#setinterface sp-4/0/0.40
```

```
user@host#set interface ms-4/2/0.40
user@host#set route-distinguisher 1:4
user@host#set vrf-import policy-1
user@host#set vrf-export policy-1
```

6. Configure a pool of the logical service interfaces that are configured in the VRF routing instances.

```
[edit]
user@host#edit services service-interface-pools pool bgf-pool
[edit services service-interface-pools pool bgf-pool]
user@host#set interface sp-4/0/0.10
user@host#set interface sp-4/0/0.20
user@host#set interface sp-4/0/0.30
user@host#set interface sp-4/0/0.40
```

7. Create a service set that links the VRF and BGF services. Specify the service interface pool name as the next-hop service. The service must contain a BGF rule. It cannot contain another rule.

```
[edit]
user@host#edit services service-set bgf
[edit services service-set bgf]
user@host#set next-hop-service service-interface-pool bgf-pool
user@host#set pgcp-rules bgf-rule
```

8. Configure the BSG service-interface.

```
[edit service border-signaling-gateway gateway bsg-1]
user@host#set service interface ms-4/2/0
```

9. Configure BSG service class.

```
[edit]
user@host#edit services border-signaling-gateway gateway bsg1 embedded-spdf
  service-class default term all
[edit services border-signaling-gateway gateway bsg1 embedded-spdf service-class
  default term all]
user@host#set from media-type any-media
user@host#set then committed-information-rate 100000
user@host#set then committed-burst-size 2000
user@host#set dscp af11
```

10. Configure BSG new transaction policies.

```
[edit]
user@host#edit services border-signaling-gateway gateway bsg1 sip
  new-transaction-policy vpn_tr_to_vlan1 term call_to_vlan1
[edit services border-signaling-gateway gateway bsg1 sip new-transaction-policy
  vpn_tr_to_vlan1 term call_to_vlan1]
user@host#set from request-uri regular-expression sip:701.*
user@host#set then accept route egress-service-point vpn_1

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 sip
  new-transaction-policy vpn_tr_to_vlan2 term call_to_vlan2
```

```
[edit services border-signaling-gateway gateway bsg1 sip new-transaction-policy
  vpn_tr_to_vlan2 term call_to_vlan2]
user@host#set from request-uri regular-expression sip:702.*
user@host#set then accept route egress-service-point vpn_2

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 sip
  new-transaction-policy vpn_tr_to_vlan3 term call_to_vlan3
[edit services border-signaling-gateway gateway bsg1 sip new-transaction-policy
  vpn_tr_to_vlan3 term call_to_vlan3]
user@host#set from request-uri regular-expression sip:703.*
user@host#set then accept route egress-service-point vpn_3

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 sip
  new-transaction-policy vpn_tr_to_vlan4 term call_to_vlan4
[edit services border-signaling-gateway gateway bsg1 sip new-transaction-policy
  vpn_tr_to_vlan4 term call_to_vlan4]
user@host#set from request-uri regular-expression sip:704.*
user@host#set then accept route egress-service-point vpn_4
```

11. Configure a new call usage policy.

```
[edit services border-signaling-gateway gateway bsg1 sip new-call-usage-policy
  call_juni_accept term accept_all]
user@host#set then accept media-policy service-class default
user@host#set new-call-usage-policies call_juni_accept
```

12. Configure NAT pools for use with BGF media services.

```
[edit]
user@host#edit services nat pool vpn_1_nat
[edit services nat pool vpn_1_nat]
user@host#set pgcp
user@host#set port automatic
user@host#set address 70.101.101.2/32

[edit]
user@host#edit services nat pool vpn_2_nat
[edit services nat pool vpn_2_nat ]
user@host#set pgcp
user@host#set port automatic
user@host#set address 70.101.102.2/32

[edit]
user@host#edit services nat pool vpn_3_nat
[edit services nat pool vpn_3 ]
user@host#set pgcp
user@host#set port automatic
user@host#set address 70.101.101.3/32

[edit]
user@host#edit services nat pool vpn_4_nat
[edit services nat pool vpn_4 ]
user@host#set pgcp
user@host#set port automatic
```

```
user@host#set address 70.101.101.4/32
```

13. Associate BGF media services with NAT pools.

```
[edit services pgcp]
user@host#set media-service vpn_1_ms nat-pool vpn_1_nat
user@host#set nat-pool vpn_1_nat_pool
user@host#set media-service vpn_2_ms nat-pool vpn_2_nat
user@host#set nat-pool vpn_2_nat_pool
user@host#set media-service vpn_3_ms nat-pool vpn_3_nat
user@host#set nat-pool vpn_3_nat_pool
user@host#set media-service vpn_4_ms nat-pool vpn_4_nat
user@host#set nat-pool vpn_4_nat_pool
```

14. Configure virtual interfaces for the BGF.

```
[edit]
user@host#edit services pgcp virtual-interface 1
[edit services pgcp virtual-interface 1]
user@host#set routing-instance vrf_1 service-interface sp-4/0/0.10
user@host#set service-state in-service media-service vpn_1_ms

[edit]
user@host#edit services pgcp virtual-interface 2
[edit services pgcp virtual-interface 2]
user@host#set routing-instance vrf_2 service-interface sp-4/0/0.20
user@host#set service-state in-service media-service vpn_2_ms

[edit]
user@host#edit services pgcp virtual-interface 3
[edit services pgcp virtual-interface 3]
user@host#set routing-instance vrf_3 service-interface sp-4/0/0.30
user@host#set service-state in-service media-service vpn_3_ms

[edit]
user@host#edit services pgcp virtual-interface 4
[edit services pgcp virtual-interface 4]
user@host#set routing-instance vrf_4 service-interface sp-4/0/0.40
user@host#set service-state in-service media-service vpn_4_ms
```

15. Configure the BSG service interface.

```
[edit services border-signaling-gateway gateway bsg1]
user@host#set service-interface ms-4/2/0
```

16. Configure BSG service points.

```
[edit]
user@host#edit services border-signaling-gateway gateway bsg1 service-point
  vpn_1
[edit services border-signaling-gateway gateway bsg1 service-point vpn_1]
user@host#set service-point-type sip transport-details port-number 5060 udp
user@host#set service-interface ms-4/2/0.10
user@host#set default-media-realm 1
user@host#edit service-policies
```

```
[edit services border-signaling-gateway gateway bsg1 service-point vpn_1
  service-policies]
user@host#set new-transaction-policies [ vpn_tr_to_vlan_2 vpn_tr_to_vlan_3
  vpn_tr_to_vlan_4 ]
user@host#set new-call-usage-policies call_juni_accept

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 service-point
  vpn_3

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 service-point
  vpn_2
[edit services border-signaling-gateway gateway bsg1 service-point vpn_2]
user@host#set service-point-type sip transport-details port-number 5060 udp
user@host#set service-interface ms-4/2/0.20
user@host#set default-media-realm 2
user@host#edit service-policies
[edit services border-signaling-gateway gateway bsg1 service-point vpn_2
  service-policies]
user@host#set new-transaction-policies [ vpn_tr_to_vlan_1 vpn_tr_to_vlan_3
  vpn_tr_to_vlan_4 ]
user@host#set new-call-usage-policies call_juni_accept

[edit services border-signaling-gateway gateway bsg1 service-point vpn_3]
user@host#set service-point-type sip transport-details port 5060 udp
user@host#set service-interface ms-4/2/0.30
user@host#set default-media-realm 3
user@host#edit service-policies
[edit services border-signaling-gateway gateway bsg1 service-point vpn_3
  service-policies]
user@host#set new-transaction-policies [ vpn_tr_to_vlan_1 vpn_tr_to_vlan_2
  vpn_tr_to_vlan_4 ]
user@host#set new-call-usage-policies call_juni_accept

[edit]
user@host#edit services border-signaling-gateway gateway bsg1 service-point
  vpn_4
[edit services border-signaling-gateway gateway bsg1 service-point vpn_4]
user@host#set service-point-type sip transport-details port-number 5060 udp
user@host#set service-interface ms-4/2/0.40
user@host#set default-media-realm 4
user@host#edit service-policies
[edit services border-signaling-gateway gateway bsg1 service-point vpn_4
  service-policies]
user@host#set new-transaction-policies [ vpn_tr_to_vlan_1 vpn_tr_to_vlan_2
  vpn_tr_to_vlan_3 ]
user@host#set new-call-usage-policies call_juni_accept
```

17. Create a BGF rule including relevant media-services

```
[edit services rule pgcp1-rule]
user@host#set gateway bgf-1 media-service [ms vpn_1_ms vpn_2_ms vpn_3_ms
  vpn_4_ms ]
```

Configuring SIP Timers

You can optionally configure two BSG SIP timers to generate timeouts.

Step-by-Step Procedure To configure SIP timers:

1. Access the SIP configuration for the BSG.

   ```
   user@host#edit services border-signaling-gateway gateway bsg-1 sip
   ```

2. Access the SIP timer function.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip]
   user@host#edit timers
   ```

3. Configure Timer C, which is the time, in seconds, the BSG waits for a final response to an INVITE request.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip timers]
   user@host#set timer-c 180
   ```

4. Configure the SIP timer that controls the maximum time, in seconds, that signalling on a call can be inactive before the call is disconnected.

   ```
   [edit services border-signaling-gateway gateway bsg-1 sip timers]
   user@host#set inactive-call 72000
   ```

Related Topics

- SIP Timers Overview on page 195
- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring QoS

Each BSG instance includes an embedded SPDF that includes one or more service classes that you can use to configure quality of service (QoS) for the BSG. Service classes contain rules that pertain to the treatment of bandwidth for various media types. After you create a service class, you apply it to a new call usage policy.

Step-by-Step Procedure To configure QoS:

1. Create a service class and assign it a name.

   ```
   [edit services border-signaling-gateway gateway bsg-1]
   user@host#edit embedded-spdf service-class video-high
   ```

2. Add a term to the service class and assign it a name.

   ```
   [edit services border-signaling-gateway gateway bsg-1 embedded-spdf service-class
     video-high]
   user@host#edit term term-1
   ```

3. Specify the type of media that you want to match to this service class.

```
[edit services border-signaling-gateway gateway bsg-1 embedded-spdf service-class
   video-high term term-1]
user@host#set from media-type video
```

4. Specify the QoS parameters or other actions to be performed on media that match this service class.

```
[edit services border-signaling-gateway gateway bsg-1 embedded-spdf service-class
   video-high term term-1]
user@host#edit then
[edit services border-signaling-gateway gateway bsg-1 embedded-spdf service-class
   video-high term term-1 then]
user@host#set committed-burst-size 3000
user@host#set committed-information-rate 20000
user@host#set dscp af21
```

5. Apply the service class to a new call usage policy.

```
[edit services border-signaling-gateway gateway bsg-1]
user@host#edit sip new-call-usage-policy core-video-peer term t1 then
```

```
[edit services border-signaling-gateway gateway bsg-1 sip new-call-usage-policy
   core-video-peer term t1 then]
user@host#set media-policy video-high
```

Related Topics

- *Chapter 31, Summary of Border Signaling Gateway Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Configuring Firewall and Intrusion Prevention System (IPS) Services for SIP Signaling Traffic

You can set up stateful firewall and IPS security services so that they are applied to SIP signaling traffic before the traffic reaches the BSG. To use this feature, group your stateful firewall rules and security policies in a service set configuration and then apply the service set to a service interface.

NOTE: The IPS feature uses the term Intrusion Detection and Prevention (IDP) to refer to its service package and its policies.

To set up this feature, complete the following tasks:

- Enabling the IDP and Stateful Firewall Service Packages on page 225
- Creating an IDP Policy on page 226
- Configuring a Stateful Firewall on page 226
- Configuring the Service Set on page 227
- Applying the Service Set to a Services Interface on page 228

Enabling the IDP and Stateful Firewall Service Packages

The JUNOS Software provides IDP and stateful firewall plug-in service packages that you can use with the IMSG to provide firewall and security services to your SIP signaling traffic.

Step-by-Step Procedure To enable the IDP and stateful firewall service packages on a PIC or DPC:

1. Determine the FPC slot number and the PIC number of the services PIC or DPC on which you want to enable the IDP and firewall service packages.

   In the following example, the FPC slot number is 0 and the PIC number is 3.

```
user@host>show chassis hardware
  Hardware inventory:
  Item           Version  Part number  Serial number     Description
  .
  .
  .
  FPC 0                                E-FPC
    PIC 0        REV 11   750-002971   RH1375            4x OC-3 SONET, MM
    PIC 1        REV 12   750-012838   DN0449            4x 1GE(LAN), IQ2
      Xcvr 0     REV 01   740-013111   8142659            SFP-T
      Xcvr 1     REV 01   740-013111   8142630            SFP-T
      Xcvr 2     REV 01   740-013111   8155199            SFP-T
      Xcvr 3     REV 01   740-013111   8154799            SFP-T
    PIC 2        REV 11   750-005724   RH2051            2x OC-3 ATM-II IQ, MM
    PIC 3        REV 15   750-014895   DN3277            MultiServices 100
  .
  .
  .
```

2. Enable the IDP and stateful firewall packages on the PIC or DPC.

```
[edit chassis]
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   package jservices-idp
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   package jservices-sfw
```

3. Set the number of megabytes that can be used for the wired process memory, which is virtual memory used to reduce Translation Look-aside Buffer (TLB) misses.

```
[edit chassis]
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   wired-process-mem-size 512
```

4. Set the number of processing cores dedicated to the control functionality of the jservices-idp and jservices-sfw applications.

```
[edit chassis]
user@host#set fpc 0 pic 3 adaptive-services service-package extension-provider
   control-cores 7
```

5. Specify that the PIC or DPC not restart if the routing engine is swapped.

```
[edit chassis]
user@host#set no-service-pic-restart-on-failover
```

6. Commit your configuration changes. You must perform the commit before you can proceed to configure the IMSG.

```
[edit]
user@host#commit
commit complete
```

Creating an IDP Policy

Step-by-Step Procedure To create an IDP policy:

1. Create an IDP policy and assign a name to it.

```
[edit security idp]
user@host#edit idp-policy attack-prevention
```

2. Create a rulebase. For example, to create an Intrusion prevention system (IPS) rulebase:

```
[edit security idp idp-policy attack-prevention]
user@host#edit rulebase-ips
[edit security idp idp-policy attack-prevention rulebase-ips]
```

3. Add rules to the rulebase.

```
[edit security idp idp-policy attack-prevention rulebase-ips]
user@host#edit rule 1
[edit security idp idp-policy attack-prevention rulebase-ips rule 1]
```

4. Define match criteria for the rule.

```
[edit security idp idp-policy attack-prevention rulebase-ips rule 1]
user@host#set match application default
user@host#set match attacks predefined-attacks [FTP:USER:ROOT
  TELNET:USER:ROOT]
```

5. Specify actions for the rule.

```
[edit security idp idp-policy attack-prevention rulebase-ips rule 1]
user@host#set then action drop-connection
user@host#set then notification log-attacks
```

Related Topics ■ *JUNOS Software Security Configuration Guide*

Configuring a Stateful Firewall

Step-by-Step Procedure To create a stateful firewall:

1. Create a stateful firewall rule.

```
[edit services stateful-firewall]
user@host#edit rule r1
```

2. Set the match direction for the rule.

```
[edit services stateful-firewall rule r1]
user@host#set match-direction input-output
```

3. Add a term to the rule.

```
[edit services stateful-firewall rule r1]
user@host#edit term t1
```

4. Configure the term.

```
[edit services stateful-firewall rule r1]
user@host#set then accept
user@host#set then syslog
```

Configuring the Service Set

Create a service set that contains the IDP policy and the stateful firewall rule.

Step-by-Step Procedure To configure a service set:

1. Create a service set configuration.

```
[edit services]
user@host#edit service-set IPS-FW
```

2. Specify the name of the stateful firewall rule that you want to apply using this service set.

```
[edit services service-set IPS-FW]
user@host#set stateful-firewall-rules r1
```

3. Specify the name of the IDP policy that you want to apply using this service set.

```
[edit services service-set IPS-FW]
user@host#set idp-profile attack-prevention
```

4. Specify the service interface on which you want the service set applied.

```
[edit services service-set IPS-FW]
user@host#set interface-service service-interface sp-0/2/0.10
```

Related Topics

- *Chapter 22, Service Set Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 23, Summary of Service Set Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Applying the Service Set to a Services Interface

In the interface that you configured for your BSG, you need to add the IDP and stateful firewall service set.

You can apply the service set to traffic received on the interface (input) and to traffic transmitted on the interface (output). However, for service sets with bidirectional service rules, you must include the same service set in both the input and output directions.

Step-by-Step Procedure To apply the service set to a service itnerface:

1. Enter edit mode for the service interface.

```
[edit]
user@host#edit interfaces ms-0/0/0
```

2. Configure a logical unit and the protocol family and enter edit mode for the logical unit.

```
[edit interfaces ms-0/0/0]
user@host#edit unit 0 family inet
```

3. Apply the service set to the input and output directions on the interface.

```
[edit interfaces ms-0/0/0 unit 0 family inet]
user@host#set service input service-set IPS-FW
user@host#set service output service-set IPS-FW
```

Related Topics

- *Chapter 24, Interface Configuration Guidelines* in *JUNOS Services Interfaces Configuration Guide*
- *Chapter 25, Summary of Interface Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Verifying the IMSG Configuration

Purpose Display the IMSG configuration.

Action

```
[edit]
user@host# show
.
.
.
system {
    processes {
        sbc-configuration-process {
            traceoptions {
                flag {
                    ipc info;
                }
            }
        }
```

```
        pgcp-service disable;
    }
}
chassis {
    no-service-pic-restart-on-failover;
    fpc 0 {
        pic 3 {
            adaptive-services {
                service-package {
                    extension-provider {
                        control-cores 1;
                        wired-process-mem-size 512;
                        package jservices-voice;
                    }
                }
            }
        }
    }
}
interfaces {
    sp-0/2/0 {
        description BGF-Service-PIC;
        services-options {
            syslog {
                host local {
                    services any;
                }
            }
        }
        unit 0 {
            family inet {
                address 10.10.200.21/32;
            }
        }
        unit 10 {
            family inet;
            service-domain inside;
        }
        unit 20 {
            family inet;
            service-domain outside;
        }
    }
    ms-0/3/0 {
        unit 0 {
            description BSG-Service-PIC;
            family inet {
                address 10.10.200.20/32;
            }
        }
    }
}

services {
    service-set bgf-svc-set {
        syslog {
            host local-1 {
                services any;
            }
        }
        stateful-firewall-rules r1;
```

```
    pgcp-rules bgf-rule-1;
    next-hop-service {
        inside-service-interface sp-0/2/0.10;
        outside-service-interface sp-0/2/0.20;
    }
}
stateful-firewall {
    rule r1 {
        match-direction input-output;
        term t1 {
            then {
                reject;
            }
        }
    }
}
pgcp {
    media-service media-service-one {
        nat-pool bsg_rtp_nat_pool;
    }
    virtual-interface 0 {
        service-state in-service;
        media-service media-service-one;
    }
    gateway bgf-1 {
        gateway-address 10.10.200.21;
        gateway-port 2944;
        service-state in-service;
        gateway-controller bsg-1 {
            controller-address 10.10.200.20;
            controller-port 2944;
            local-controller bsg-1;
        }
        platform {
            device ms-0/3/0;
        }
    }
    rule bgf-rule-1 {
        gateway bgf-1;
        media-service media-service-one;
    }
}
border-signaling-gateway {
    gateway bsg-1 {
        service-interface ms-0/3/0;
        sip {
            timers {
                inactive-call 72000;
                timer-c 180;
            }
            new-transaction-policy emergency-call-route {
                term t1 {
                    from {
                        request-uri {
                         regular-expression "sip:9[0-9]+@.+ | tel:9[0-9])+";

                        }
                    }
                    then {
                        route {
                            next-hop {
```

```
                        address 196.10.3.45 port 5060;
                    }
                    egress-service-point sip-udp-5060;
                }
            }
        }
    }
    new-transaction-policy peer-2-core;
    new-transaction-policy policy10 {
        term peer-to-peer {
            then {
                admission-control acprofile1;
            }
        }
    }
    new-transaction-policy-set peer-to-core {
        policy-name [ emergency-call-route peer-2-core ];
    }
    new-call-usage-policy peer-media-2-core {
        term voice {
            from {
                request-uri {
                    regular-expression sip:555.+;
                }
            }
            then {
                media-policy {
                    service-class voice-high;
                }
            }
        }
        term video {
            from {
                request-uri {
                    regular-expression sip:121.+;
                }
            }
            then {
                media-policy {
                    service-class video-high;
                }
            }
        }
    }
}
admission-control acprofile1 {
    dialogs {
        maximum-concurrent 50000;
        committed-attempts-rate 50;
        committed-burst-size 100;
    }
    transactions {
        maximum-concurrent 50000;
        committed-attempts-rate 50;
        committed-burst-size 100;
    }
}
service-point sip-udp-5060 {
    service-point-type sip;
    transport-details port-number 5060 ip-address 10.10.200.20 udp;
    service-interface ms-0/3/0;
```

```
                    service-policies {
                        new-transaction-policies peer-to-core;
                        new-call-usage-policies peer-media-2-core;
                    }
                }
                embedded-spdf {
                    service-class video-high {
                        term term-1 {
                            from {
                                media-type video;
                            }
                            then {
                                committed-information-rate 20000;
                                committed-burst-size 2000;
                                dscp af21;
                            }
                        }
                    }
                    service-class voice-high {
                        term t-1 {
                            from {
                                media-type audio;
                            }
                            then {
                                committed-information-rate 20000;
                                committed-burst-size 10000;
                                dscp af21;
                            }
                        }
                    }
                }
            }
        }
        nat {
            pool bsg_rtp_nat_pool {
                pgcp {
                    ports-per-session 2;
                }
                address-range low 10.10.20.100 high 10.10.30.100;
                port automatic;
            }
        }
    }
```

Chapter 13

Monitoring the IMSG

This chapter explains how to monitor IMSG components. Topics include:

Monitoring Call Statistics

Purpose Display statistics for calls on a specific BSG using the show services border-signaling-gateway calls gateway *gateway-name* command.

Action

```
user@host> show services border-signaling-gateway calls gateway bsg-1
Statistics Start    : 06-02-2009  15:25:48.

            Service Point       : 10_100_100_20-5060
            Direction           : Egress
            Failed Calls        : 0
            Active Calls        : 1
            Completed Calls     : 0

            Service Point       : 10_100_100_20-5060
            Direction           : Ingress
            Failed Calls        : 14
            Active Calls        : 1
            Completed Calls     : 0
```

Related Topics

- *Chapter 16, Border Signaling Gateway Operational Mode Commands* in *JUNOS System Basics and Services Command Reference*

Monitoring Statistics for Failed Calls

Purpose Display statistics for calls that have failed on a specific BSG using the show services border-signaling-gateway calls-failed gateway *gateway-name* command.

Action

```
user@host> show services border-signaling-gateway calls-failed gateway bsg-1

  Statistics Start    : 05-06-2009  12:22:03.
```

```
Service Point                          : sip-5060-udp
   Direction                             : Egress
   Protocol Error                        : 0
   Inactive Timeout                      : 0
   Configured Behavior Policy Rejection  : 0
   4/5/6XX Response                      : 0

   Service Point                         : sip-5060-udp
   Direction                             : Ingress
   Protocol Error                        : 0
   Inactive Timeout                      : 0
   Configured Behavior Policy Rejection  : 0
   4/5/6XX Response                      : 0

   Service Point                         : sip-5060-tcp
   Direction                             : Egress
   Protocol Error                        : 0
   Inactive Timeout                      : 0
   Configured Behavior Policy Rejection  : 0
   4/5/6XX Response                      : 0

   Service Point                         : sip-5060-tcp
   Direction                             : Ingress
   Protocol Error                        : 0
   Inactive Timeout                      : 0
   Configured Behavior Policy Rejection  : 0
```

Related Topics

- *Chapter 16, Border Signaling Gateway Operational Mode Commands* in *JUNOS System Basics and Services Command Reference*

Monitoring Call Information for a Specific Contact

Purpose Display call information about a specific contact using the show services border-signaling-gateway by-contact *contact* gateway *gateway-name* command.

Action

```
user@host> run show services border-signaling-gateway by-contact
<sip:5555@10.10.0.100:5060> gateway BSG1 detail
Signaling Source IP       : 10.100.100.20
Signaling Destination IP  : 10.10.0.100
Call-ID                   : CALL_ID1_001B11976D2A_T1993314563@10.10.0.100
Local URI                 : 10.100.100.20
Remote URI                : <sip:5555@10.10.0.100:5060>
Local Tag                 : bsg+1000003+11a0000+3b3fc23da6bbfa474
Remote Tag                : 001B11976D2A_T15367637774
Next Hop                  : According to SIP protocol
Admission Control Profile : acprofile1
Manipulation Rules         : ManipulationTowardsPeer1, HM_rule_2
Media IP                  : 10.10.0.100
Media Port                : 41000
Media Status              : Enabled
```

Related Topics
- *Chapter 16, Border Signaling Gateway Operational Mode Commands* in *JUNOS System Basics and Services Command Reference*

Monitoring Call Information for a Specific Request URI

Purpose Display call information for a specific request URI using the show services border-signaling-gateway by-request-uri *request-uri* gateway *gateway-name* command.

Action

```
user@host> run show services border-signaling-gateway by-request-uri
"sip:3636@10.100.100.20:5060" gateway BSG1 detail
Signaling Source IP       : 10.100.100.20
Signaling Destination IP  : 10.10.0.100
Call-ID                   : CALL_ID1_001B11976D2A_T1993314563@10.10.0.100
Local URI                 : 10.100.100.20
Remote URI                : <sip:5555@10.10.0.100:5060>
Local Tag                 : bsg+1000003+11a0000+3b3fc23da6bbfa474
Remote Tag                : 001B11976D2A_T15367637774
Next Hop                  : According to SIP protocol
Admission Control Profile : acprofile1
Manipulation Rules        : ManipulationTowardsPeer1, HM_rule_2
Media IP                  : 10.10.0.100
Media Port                : 41000
Media Status              : Enabled
```

Related Topics
- *Chapter 16, Border Signaling Gateway Operational Mode Commands* in *JUNOS System Basics and Services Command Reference*

Monitoring Call Admission Control (CAC) Statistics

Purpose Display statistics for CAC using the show services border-signaling-gateway admission-control gateway *gateway-name* command.

Action

```
user@host> show services border-signaling-gateway admission-control gateway bsg-1
Admission control profile: acprofile1
  Dialogs
    Active: 2% (20 out of 1000 allowed)
    Attempts handled: 5500
    Attempts rejected due to concurrent exception: 2
    Attempts rejected due to rate exception: 4
  Transactions
    Active: 0% (10 out of 50000 allowed)
    Attempts handled: 20000
    Attempts rejected due to concurrent exception: 10
    Attempts rejected due to rate exception: 1
```

Related Topics
- *Chapter 16, Border Signaling Gateway Operational Mode Commands* in *JUNOS System Basics and Services Command Reference*

Chapter 14

Managing the IMSG

This chapter describes how to manage components on the IMSG. Topics include:

Activating and Deactivating BSG Services

This topic describes the process of deactivating and activating BSG services.

Activating BSG Services

To activate BSG services, enter the activate services border-signaling-gateway statement in configuration mode, and then commit your configuration:

```
[edit]
user@host# activate services border-signaling-gateway
user@host# commit
```

Deactivating BSG Services

To deactivate BSG services, enter the deactivate services border-signaling-gateway statement in configuration mode, and then commit your configuration:

```
[edit]
user@host# deactivate services border-signaling-gateway
user@host# commit
```

Managing the SBC Configuration Process

You can stop and start the SBC configuration process in any or these ways:

- Restart the SBC configuration process. In this procedure, the SBC configuration process is considered configured.
- Disable and enable the SBC configuration process. In this procedure, the SBC configuration process is considered configured.
- Activate and deactivate the SBC configuration process.

Restarting the SBC Configuration Process

CAUTION: We recommend that you do not restart the software process unless instructed to do so by a Juniper Networks customer support engineer. A restart might cause the router to drop calls and interrupt transmission.

Three options are available when you restart the SBC configuration process:

- gracefully—Restart the software process after calls have ended.
- immediately—Immediately restart the software process.
- soft—Reread and reactivate the configuration without completely restarting the software process.

To restart the SBC configuration process, enter the restart sbc-configuration-process command in operational mode:

```
user@host>restart sbc-configuration-process
```

When you restart the SBC configuration process, the process is stopped and then restarted.

Disabling and Enabling the SBC Configuration Process

This topic describes the process of disabling and enabling the SBC configuration process.

Disabling the SBC Configuration Process

To disable the SBC configuration process, enter the set system processes sbc-configuration-process disable statement in configuration mode, and then commit your configuration:

```
[edit]
user@host# set system processes sbc-configuration-process disable
user@host# commit
```

Enabling the SBC Configuration Process

To enable the SBC configuration process, enter the delete system processes sbc-configuration-process disable statement in configuration mode, and then commit your configuration:

```
[edit]
user@host# delete system processes sbc-configuration-process disable
user@host# commit
```

Chapter 15

Troubleshooting the IMSG

This chapter explains how to set up trace options for the IMSG. Topics include:

Tracing Border Signaling Gateway Operations

You can trace the following BSG components and record trace results in a log file:

- datastore
- framework
- session trace
- SBC utilities
- signaling
- SIP stack

All log files are placed in the /var/log directory. When a trace file reaches its maximum size, a .0 is appended to the filename, then a new file is created with a .1 appended, and so on. When the maximum number of trace files is reached, the oldest trace file is overwritten.

Step-by-Step Procedure To configure tracing of BSG operations:

1. Access the traceoptions configuration.

   ```
   [edit]
   user@host# edit services border-signaling-gateway gateway bsg1 traceoptions
   [edit services border-signaling-gateway traceoptions]
   ```

2. Access the traceoptions trace file configuration.

   ```
   [edit services border-signaling-gateway traceoptions]
   user@host# edit file
   [edit services border-signaling-gateway traceoptions file]
   ```

3. Specify a name for the trace file.

   ```
   [edit services border-signaling-gateway traceoptions file]
   user@host# set filename bsg1
   ```

4. Set the maximum number of trace files.

```
[edit services border-signaling-gateway traceoptions file]
user@host# set files 10
```

5. Set user access to the trace log file. Use set no-world-readable to prevent users from accessing the log file, or use set world-reabable to allow any user to read the log file.

```
[edit services pgcp traceoptions file]
user@host# set no-world-readable
```

6. Access the traceoptions flag configuration to define trace level options.

```
[edit services border-signaling-gateway traceoptions file]
user@host# up
[edit services border-signaling-gateway traceoptions]
user@host# edit flag
```

7. Set trace level options for any other components for which you do not want the default level, error. For example:

```
[edit services border-signaling-gateway traceoptions flag]
user@host# set datastore debug
[edit services border-signaling-gateway traceoptions flag]
user@host# set signaling policy warning
[edit services border-signaling-gateway traceoptions flag]
user@host# set SBC-utils memory-management debug
[edit services border-signaling-gateway traceoptions flag]
user@host# set sip-stack event-tracing
[edit services border-signaling-gateway traceoptions flag]
user@host# set sip-stack pd-log-level audit
[edit services border-signaling-gateway traceoptions flag]
```

Related Topics

- *Chapter 27, Summary of PGCP Configuration Statements* in *JUNOS Services Interfaces Configuration Guide*

Tracing the SBC Configuration Process

You can trace the following SBC configuration process events and record trace results in a log file:

- common
- configuration
- device monitor
- IPC
- memory pool
- user interface

All log files are placed in the /var/log directory. When a trace file reaches its maximum size, a .0 is appended to the filename, then a new file is created with a .1 appended, and so on. When the maximum number of trace files is reached, the oldest trace file is overwritten.

Step-by-Step Procedure To configure tracing of the SBC configuration process:

1. Access the traceoptions configuration.

```
[edit]
user@host# edit system processes sbc-configuration-process traceoptions
[edit system processes sbc-configuration-process traceoptions]
```

2. Access the traceoptions trace file configuration.

```
[edit system processes sbc-configuration-process traceoptions]
user@host# edit file
[edit system processes sbc-configuration-process traceoptions file]
```

3. Specify a name for the trace file.

```
[edit system processes sbc-configuration-process traceoptions file]
user@host# set filename sbc-config-trace
```

4. Set the maximum number of trace files.

```
[edit system processes sbc-configuration-process traceoptions file]
user@host# set files 10
```

5. Set user access to the trace log file. Use set no-world-readable to prevent users from accessing the log file, or use set world-reabable to allow any user to read the log file.

```
[edit system processes sbc-configuration-process traceoptions file]
user@host# set no-world-readable
```

6. Access the traceoptions flag configuration to define trace level options.

```
[edit system processes sbc-configuration-process traceoptions file]
user@host# up
[edit system processes sbc-configuration-process traceoptions]
user@host# edit flag
```

7. Set trace level options for the components of the SBC configuration process that you want to trace. For example:

```
[edit system processes sbc-configuration-process traceoptions flag]
user@host# set common debug
[edit system processes sbc-configuration-process traceoptions flag]
user@host# set configuration debug
[edit system processes sbc-configuration-process traceoptions flag]
user@host# set memory-pool debug
```

Part 4
Index

Index

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W