JUNOS® Software

Broadband Subscriber Management Solutions Guide

Release 9.5

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

Part Number: 530-029389-01, Revision 1

JUNOS® Software Broadband Subscriber Management Solutions Guide
Release 9.5

Writing: Mark Barnard
Editing: Ben Mann
Illustration: Nathaniel Woodward, Mark Barnard
Cover Design: Edmonds Design

Revision History
13 April 2009—530-029389-01 Revision 1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

List of Figures

List of Tables

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software Broadband Subscriber Management 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 *JUNOS Release Notes* differs from the information in the documentation, follow the *JUNOS Release Notes*.

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

Table 1 on page xv lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at http://www.juniper.net/books.

Table 1: Additional Books Available Through http://www.juniper.net/books

Book	Description
Interdomain Multicast Routing	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.

Table 1: Additional Books Available Through http://www.juniper.net/books *(continued)*

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

Objectives

This guide provides an overview of broadband subscriber management using JUNOS software and describes how to configure and manage remote subscribers on the routing platform.

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 MX-series routing platform.

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

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)

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

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

Supported Routing Platforms

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

- MX-series

Using the Indexes

This reference contains a complete index that includes topic entries.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the load merge or the load merge relative command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the load merge command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the load merge relative command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file ex-script.conf. Copy the ex-script.conf file to the /var/tmp directory on your routing platform.

```
system {
    scripts {
        commit {
            file ex-script.xsl;
        }
    }
}
interfaces {
    fxp0 {
        disable;
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
        }
    }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the load merge configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file ex-script-snippet.conf. Copy the ex-script-snippet.conf file to the /var/tmp directory on your routing platform.

```
commit {
    file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the load merge relative configuration mode command:

```
[edit system scripts]
```

```
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the load command, see the *JUNOS CLI User Guide*.

Documentation Conventions

Table 2 on page xix defines notice icons used in this guide.

Table 2: 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 3 on page xix defines the text and syntax conventions used in this guide.

Table 3: 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*

Table 3: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;
| (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

Broadband Subscriber Management Overview

Chapter 1

Subscriber Management Basics Overview

Broadband Subscriber Management Overview

Broadband Subscriber Management is a method of dynamically provisioning and managing subscriber access in a multiplay or triple play network environment. This method uses AAA configuration in conjunction with dynamic profiles to provide dynamic, per-subscriber authentication, addressing, access, and configuration for a host of broadband services including Internet access, gaming, IPTV, Video on Demand (VoD), and subscriber wholesaling.

NOTE: The JUNOS broadband subscriber management solution currently supports only DHCP-based configuration and RADIUS authentication and authorization.

This guide focuses on the general components necessary for configuring a Juniper Networks MX-series Ethernet Services router to dynamically provision and manage subscribers. However, you can also use a Juniper Networks EX-series Ethernet Switch in a subscriber network.

Managing subscribers in a DHCP-based residential broadband network using a Juniper Networks MX-series router requires the following:

- Planning and configuring a virtual LAN (VLAN) architecture for the access network.
- Configuring an authentication, authorization, and accounting (AAA) framework for subscriber authentication and authorization through external servers (for example, RADIUS) as well as accounting and dynamic-request change of authorization (CoA) and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS.
- Configuring DHCP local server or DHCP relay for subscriber address assignment.

- Configuring dynamic profiles to include dynamic IGMP, firewall filter, and class of service (CoS) configuration for subscriber access.
- Configuring multicast access to the core network.

To better understand the subscriber access network, this guide also provides general information about some hardware not from Juniper Networks and suggests methods for choosing different network configuration options. You can configure a subscriber network in many different ways. This guide does not cover all configuration scenarios. It is intended as a starting point for understanding subscriber management and how you can use Juniper Networks hardware and software to plan and build your own subscriber management solution.

Related Topics

- Broadband Subscriber Management Platform Support on page 4
- Broadband Subscriber Management Network Topology Overview on page 4
- Broadband Subscriber Management Solutions Terms and Acronyms on page 5
- Supporting Documentation for Broadband Subscriber Management on page 7
- Triple Play and Multiplay Overview on page 7
- Broadband History on page 9

Broadband Subscriber Management Platform Support

Juniper Networks currently supports broadband subscriber management solutions only on MX-series routers.

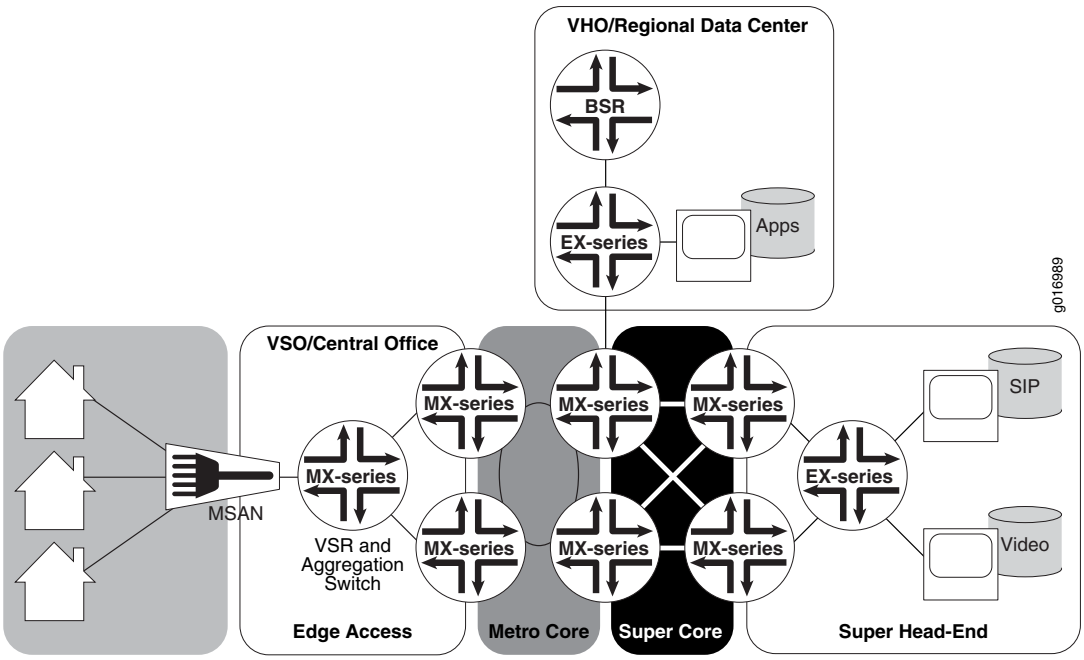
Related Topics

- Broadband Subscriber Management Overview on page 3
- Broadband Subscriber Management Edge Router Overview on page 15

Broadband Subscriber Management Network Topology Overview

Figure 1 on page 5 illustrates how network elements can make up a residential broadband access network.

Figure 1: Subscriber Management Residential Broadband Network Example



Related Topics

- Broadband Subscriber Management Overview on page 3

Broadband Subscriber Management Solutions Terms and Acronyms

- **AAA (authentication, authorization, and accounting)**—An IP-based networking system that controls user access to computer resources and manages the activity of users over a network.
- **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.
- **CoA (change of authorization)**—RADIUS messages that contain information for dynamically changing session authorizations.
- **CoS (class of service)**—A method of managing network traffic by grouping similar types of traffic together and treating each traffic type as a “class” with a defined service priority.
- **DHCP (Dynamic Host Configuration Protocol)**—A networking protocol used by subscribers to obtain the addressing information necessary for operation in an Internet Protocol (IP) network.
- **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.
- **MSAN (Multiservice Access Node)**—A group of commonly used aggregation devices including digital subscriber line access multiplexers (DSLAMs) used in xDSL networks, optical line termination (OLT) for PON/FTTx networks, and Ethernet switches for Active Ethernet connections.
- **Multiplay**—A networking paradigm that enables the ability to add new and robust networking services that individual subscriber can access.
- **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.
- **RADIUS (Remote Authentication Dial In User Service)**—A networking protocol that provides centralized access, authorization, and accounting management for subscribers to connect and use a network service.
- **Residential 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.
- **Triple play**—A networking paradigm that dedicates bandwidth to data, voice, and video service.
- **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 video services router is any M-series or MX-series router that supports the video routing package provided with JUNOS software Release 8.3 or later.

Related Topics
- Broadband Subscriber Management Overview on page 3

Supporting Documentation for Broadband Subscriber Management

The *JUNOS Broadband Subscriber Management Solutions Guide* relies heavily on existing configuration documentation. In particular, this guide references configuration material presented in the *JUNOS Subscriber Access Configuration Guide*. We recommend you become familiar with the configuration options presented for subscriber access before reading this guide.

Several guides in the JUNOS software documentation set provide detailed configuration information that is not fully covered in this guide. This guide might reference other JUNOS software configuration and solutions documents that can provide more detail about a specific feature or configuration option.

For more detailed configuration information, see the following JUNOS software documents:

- *JUNOS Subscriber Access Configuration Guide*
- *JUNOS MX-series Layer 2 Configuration Guide*
- *JUNOS Multicast Protocols Configuration Guide*
- *JUNOS Network Interfaces Configuration Guide*
- *JUNOS Policy Framework Configuration Guide*

For other solution examples, see the following JUNOS software solutions guides:

- *JUNOS MX-series Solutions Guide*
- *JUNOS Multiplay Solutions Guide*

In addition to related JUNOS documentation, you can obtain useful information from the JUNOSe software documentation. Many features described in the *JUNOSe Broadband Access Configuration Guide* are similar to those described in both this guide and the *JUNOS Subscriber Access Configuration Guide*.

Related Topics
- Broadband Subscriber Management Overview on page 3

Triple Play and Multiplay Overview

This document defines triple play and multiplay networks as different entities:

- A *triple play* network dedicates bandwidth to each possible service—data, voice, and video. This method works well when a limited number of services are deployed and sufficient bandwidth is available.
- A *multiplay* network refers to the ability to add new and robust networking services that each subscriber can access. This method requires the integration of dynamic bandwidth management and the ability to manage subscribers dynamically though the use of features such as hierarchical quality of service

(QoS) and a AAA service framework that provides authentication, accounting, dynamic change of authorization (CoA), and dynamic address assignment.

Table 4 on page 8 provides some comparison between a triple play and multiplay network and the level of flexibility associated with certain networking options.

Table 4: Triple Play and Multiplay Comparison

Flexibility	Triple Play	Multiplay
Bandwidth Management	Fixed bandwidth allocation for each service.	One bandwidth pool for each subscriber is shared by all services.
Adding New Services	Requires *deallocating* bandwidth from one service and allocating that bandwith to the new service.	The existence of one shared bandwidth pool eliminates the need to reallocate bandwidth to new services.
Subscriber Flexibility	Limited subscriber flexibility because a fixed bandwidth is allocated to each service or application.	Subscribers can use their share of bandwidth for whatever applications they want to run.
Client Device Types	Client devices (PCs or set-top boxes) are dedicated to specific services and often assigned to specific ports on customer premise equipment.	Client devices are not assigned to any specific ports. This flexibility enables the ability to use client devices for various services (for example, adding software to a PC to enable television broadcasts) and allows different client devices (PCs, Voice-over-IP phones, and set-top boxes) to reside on a single LAN.

With software and hardware now available to enable client devices to access and use the network in a variety of ways, bandwidth demands increasing, and new networking business models emerging, dynamic support of new applications is required to ensure subscriber satisfaction. A dynamic multiplay network configuration can provide the flexibility to meet these demands.

Related Topics

- Broadband Subscriber Management Overview on page 3

Chapter 2

Residential Broadband Technology Overview

Broadband History

Residential broadband services developed using a mainly ATM-based infrastructure and early Internet access required that each subscriber access the network using a dial-up modem to connect from a PC to a Remote Access Server (RAS), or bank of servers, which was connected directly to the Internet. Point-to-Point Protocol (PPP), originally defined by the IETF in RFC 1661, was already in use on leased lines. It was well suited for use on the existing ATM infrastructure and enabled operators to better manage subscriber connections by providing authentication and accounting, along with a level of protocol flexibility due to it being connection-oriented and enabling service providers to customize it to their needs. The use of the PPP model, however, required special software (including the PPP protocol stack) be installed on each PC to communicate within the PPP network. After establishing a connection to the Internet, the subscriber logged in using a PPP user identifier provided by the service provider.

This *always on* model quickly evolved in several ways. Dedicated *broadband* access such as DSL replaced dial-up service, replacing the dial-up modem with a DSL modem. Dial-up remote access servers were replaced by the Broadband Remote Access Server (B-RAS) and residential gateways were introduced to allow multiple PCs from one site to connect to the broadband network. Residential gateways have since evolved to provide a wide range of functions including firewall and wireless (802.1b/g/n wi-fi) connectivity. The residential gateway also became the termination point for the PPP connection, eliminating the need for the installation of special PC software.

These new broadband networks were built based on the following two key assumptions:

- Only a small percentage of subscribers were expected to be using network bandwidth at any given time and, even if many subscribers logged in to the network concurrently, few subscribers were likely to enter data at the exact same time.

- Traffic was TCP-based and not real-time. If a packet was lost due to network congestion, TCP detected the loss and retransmitted the packets.

Based on these assumptions, operators over-subscribed the network, enabling more subscribers than a limited amount of bandwidth can support if all subscribers were to access the network simultaneously. For example, if 50 subscribers were to sign up for service that required bandwidth of 1 Mbps for each subscriber, the network did not necessarily need to support a full 50 Mbps of throughput. Instead, operators designed the network to support much lower traffic volumes, expecting maximum traffic flow for all subscribers to occur rarely, if ever. For example, a 50:1 over-subscription needed to support only 1 Mbps of bandwidth. Bandwidth requirements have changed significantly over the years and this method of access is becoming more difficult to maintain.

The basic broadband architecture was initially defined by DSL Forum TR-025 (November 1999). This specification assumed only one service was provided to subscribers—Internet Access (or *data*). DSL Forum TR-059 (September 2003) introduced quality of service (QoS) to allow broadband networks to deliver voice over IP (VoIP) in addition to data. Because VoIP is a small percentage of overall network traffic, its introduction has not significantly altered the broadband delivery landscape. It is also worth noting that these original standards specified ATM as the Layer 2 protocol on the broadband network.

Related Topics

- DHCP in Broadband Networks on page 10
- Broadband Service Delivery Options on page 11
- Broadband Delivery and FTTx on page 12

DHCP in Broadband Networks

Dynamic Host Configuration Protocol (DHCP) is an alternative to PPP for assigning IP addresses and provisioning services in broadband networks. Using DHCP helps to simplify network configuration by decreasing (and in some cases eliminating) the need for manually configuring static IP addresses on network devices. For example, DHCP enables PCs and other devices within a subscriber residence to obtain IP addresses to access the Internet. Due to its general simplicity and scalability, along with the increased usage of Ethernet in access networks, DHCP deployments in broadband networks have increased.

NOTE: The JUNOS subscriber management solution currently supports only DHCP as a multiple-client configuration protocol. This guide provides only DHCP-based configuration examples where applicable.

Related Topics ■ Broadband Service Delivery Options on page 11

Broadband Service Delivery Options

Four primary delivery options exist today for delivering broadband network service. These options include the following:

- Digital Subscriber Line
- Active Ethernet
- Passive Optical Networking
- Hybrid Fiber Coax

The following sections briefly describe each delivery option.

Digital Subscriber Line

Digital subscriber line (DSL) is the most widely deployed broadband technology worldwide. This delivery option uses existing telephone lines to send broadband information on a different frequency than is used for the existing voice service. Many generations of DSL are used for residential service, including Very High Speed Digital Subscriber Line 2 (VDSL2) and versions of Asymmetric Digital Subscriber Line (ADSL, ADSL2, and ADSL2+). These variations of DSL primarily offer asymmetric residential broadband service where different upstream and downstream speeds are implemented. (VDSL2 also supports symmetric operation.) Other DSL variations, like High bit rate Digital Subscriber Line (HDSL) and Symmetric Digital Subscriber Line (SDSL), provide symmetric speeds and are typically used in business applications.

The head-end to a DSL system is the Digital Subscriber Line Access Multiplexer (DSLAM). The demarcation device at the customer premise is a DSL modem. DSL service models are defined by the Broadband Forum (formerly called the DSL Forum).

Active Ethernet

Active Ethernet uses traditional Ethernet technology to deliver broadband service across a fiber-optic network. Active Ethernet does not provide a separate channel for existing voice service, so VoIP (or TDM-to-VoIP) equipment is required. In addition, sending full-speed (10 or 100 Mbps) Ethernet requires significant power, necessitating distribution to Ethernet switches and optical repeaters located in cabinets outside of the central office. Due to these restrictions, early Active Ethernet deployments typically appear in densely populated areas.

Passive Optical Networking

Passive Optical Networking (PON), like Active Ethernet, uses fiber-optic cable to deliver services to the premises. This delivery option provides higher speeds than DSL but lower speeds than Active Ethernet. Though PON provides higher speed to each subscriber, it requires a higher investment in cable and connectivity.

A key advantage of PON is that it does not require any powered equipment outside of the central office. Each fiber leaving the central office is split using a non-powered optical splitter. The split fiber then follows a point-to-point connection to each subscriber.

PON technologies fall into three general categories:

- ATM PON (APON), Broadband PON (BPON), and Gigabit-capable PON (GPON)—PON standards that use the following different delivery options:
  - APON—The first passive optical network standard and is primarily used for business applications.
  - BPON—Based on APON, BPON adds wave division multiplexing (WDM), dynamic and higher upstream bandwidth allocation, and a standard management interface to enable mixed-vendor networks.
  - GPON—The most recent PON adaptation, GPON is based on BPON but supports higher rates, enhanced security, and a choice of which Layer 2 protocol to use (ATM, Generic Equipment Model [GEM], or Ethernet).
- Ethernet PON (EPON)—Provides capabilities similar to GPON, BPON, and APON, but uses Ethernet standards. These standards are defined by the IEEE. Gigabit Ethernet PON (GEPON) is the highest speed version.
- Wave Division Multiplexing PON (WDM-PON)—A nonstandard PON which, as the name implies, provides a separate wavelength to each subscriber.

The head-end to a PON system is an Optical Line Terminator (OLT). The demarcation device at the customer premises is an Optical Network Terminator (ONT). The ONT provides subscriber-side ports for connecting Ethernet (RJ-45), telephone wires (RJ-11) or coaxial cable (F-connector).

Hybrid Fiber Coaxial

Multi-System Operators (MSOs; also known as *cable TV operators*) offer broadband service through their hybrid fiber-coaxial (HFC) network. The HFC network combines optical fiber and coaxial cable to deliver service directly to the customer. Services leave the central office (CO) using a fiber-optic cable. The service is then converted outside of the CO to a coaxial cable *tree* using a series of optical nodes and, where necessary, through a trunk radio frequency (RF) amplifier. The coaxial cables then connect to multiple subscribers. The demarcation device is a cable modem or set-top box, which talks to a Cable Modem Termination System (CMTS) at the MSO *head-end* or master facility that receives television signals for processing and distribution. Broadband traffic is carried using the Data Over Cable Service Interface Specification (DOCSIS) standard defined by CableLabs and many contributing companies.

Related Topics
- Broadband Delivery and FTTx on page 12

Broadband Delivery and FTTx

Many implementations use existing copper cabling to deliver signal to the premises, but fiber-optic cable connectivity is making its way closer to the subscriber. Most

networks use a combination of both copper and fiber-optic cabling. The term *fiber to the x* (FTTx) describes how far into the network fiber-optic cabling runs before a switch to copper cabling takes place. Both PON and Active Ethernet can use fiber-optic portion of the network, while xDSL is typically used on the copper portion. This means that a single fiber-optic strand may support multiple copper-based subscribers.

Increasing the use of fiber in the network increases cost but it also increases network access speed to each subscriber.

The following terms are used to describe the termination point of fiber-optic cable in a network:

- Fiber to the Premises (FTTP), Fiber to the Home (FTTH), Fiber to the Business (FTTB)—Fiber extends all the way to the subscriber. PON is most common for residential access, although Active Ethernet can be efficiently used in dense areas such as apartment complexes. Active Ethernet is more common for delivering services to businesses.
- Fiber to the Curb (FTTC)—Fiber extends most of the way (typically, 500 feet/150 meters or less) to the subscriber. Existing copper is used for the remaining distance to the subscriber.
- Fiber to the Node/Neighborhood (FTTN)—Fiber extends to within a few thousand feet of the subscriber and converted to xDSL for the remaining distance to the subscriber.
- Fiber to the Exchange (FTTE)—A typical central office-based xDSL implementation in which fiber is used to deliver traffic to the central office and xDSL is used on the existing local loop.

Related Topics

- Broadband Service Delivery Options on page 11

Chapter 3

Broadband Subscriber Management Solution Hardware Overview

Broadband Subscriber Management Edge Router Overview

The edge router is the demarcation point between the residential broadband access network and the core network. The Juniper Networks MX-series router (along with the Juniper Networks EX-series Ethernet Switch) can play multiple roles as an edge router. The most common include the following:

- **Broadband services router (BSR)**—This router supports high speed Internet access along with several other subscriber-based services including VoIP, IPTV, and gaming.
- **Video services router (VSR)**—The video services router capabilities are a subset of those provided by a broadband services router. In general, using the MX-series router as a video services router provides bi-directional traffic destined for the set-top box (STB). This traffic includes IPTV and video on demand (VoD) streams as well as associated control traffic such as IGMP and electronic program guide (EPG) updates.

You can also use the MX-series router in certain Layer 2 solutions. For information about configuring the MX-series router in Layer 2 scenarios, see the *MX-series Layer 2 Configuration Guide* or the *MX-series Solutions Guide*.

Broadband Services Router Overview

A broadband services router is an edge router that traditionally supports primarily Internet-bound traffic. This router replaces and provides a superset of the functionality provided by a Broadband Remote Access Server (B-RAS). The broadband services router functions can be broken into two key areas—high speed Internet access and IPTV support.

High-Speed Internet Access Support

The broadband services router communicates with the RADIUS server to enforce which services each subscriber can access. For example, one subscriber might have signed up for a smaller Internet access service of 1 Mbps where another subscriber might have signed up for a higher, 10 Mbps service. The broadband services router manages the traffic to each subscriber, ensuring that each subscriber obtains the level of access service they have purchased, while also ensuring that any VoIP traffic receives priority. The broadband services router also makes traffic forwarding decisions based on aggregate bandwidth detected on any adjacent Multiservice Access Node (MSAN).

IPTV Support

The broadband services router supports IPTV traffic including support for IGMP multicast group start and stop requests from downstream MSANs. The broadband services router manages the bandwidth allocations associated with high-bandwidth IPTV as well as video on demand (VoD) traffic to ensure high quality service delivery.

Video Services Router

When configuring a multiedge network, you can use the MX-series router as a video services router (VSR) to support only video traffic without supporting the high-speed Internet access (HSIA) capabilities.

NOTE: We recommend a single-edge network model but the MX-series router allows for flexibility when defining a multiplay network topology.

Some advantages of using a separate video services router for video traffic include the following:

- Provides the ability to add IPTV service without the need to modify an existing edge router that is performing other functions.
- Reduces network bandwidth by moving the video edge further out to the network edge while still allowing for centralized broadband services router operation.
- Typically requires less capital investment because the video services router does not need to provide per-subscriber management.

Services Router Placement

Depending on the type of network you are creating—single edge or multiedge—you can place a broadband services router or video services router in various locations.

Single Edge Placement

In a single edge network, you use only broadband services routers because the single device must perform all of the necessary edge functions—providing subscriber management for high-speed Internet access and IPTV services. You can use the two following topology models when placing the broadband services router:

- **Centralized single edge**—The edge router is centrally located and placed at one location to cover a particular region. A secondary router is sometimes placed in this location to act as a backup. Downstream MSANs are connected to the broadband services router using a ring or mesh topology.
- **Distributed single edge**—The edge router is placed further out into the network, typically in the central office (CO) closest to the subscribers it services. Downstream MSANs are typically connected directly to the broadband services router (in a true, single edge topology) or through an Ethernet aggregation switch.

In general, the addition of IPTV service favors a more distributed model because it pushes the need for subscriber management farther out into the network.

Multiedge Placement

In a multiedge network, you use both broadband services routers and video services routers. The broadband services router controls any high-speed Internet traffic and the video services router controls video traffic. You can use the two following topology models when placing service routers in a multiedge network topology:

- **Co-located multiedge**—The broadband services router and video services router are housed in the same location and an Ethernet switch directs traffic in the CO to the appropriate edge router.

NOTE: A single MX–series router can serve as both Ethernet switch and video services router. For information about configuring the MX-series router in Layer 2 scenarios, see the *MX-series Layer 2 Configuration Guide* or the *MX-series Solutions Guide*.

- **Split multiedge**—The video services router and broadband services router reside in different locations. In this model, the broadband services router is typically located more centrally and video services routers are distributed.

Related Topics

- Multiservice Access Node Overview on page 17
- Ethernet MSAN Aggregation Options on page 19
- Broadband Subscriber Management Platform Support on page 4

Multiservice Access Node Overview

A *multiservice access node* is a broader term that refers to a group of commonly used aggregation devices. These devices include digital subscriber line access multiplexers (DSLAMs) used in xDSL networks, optical line termination (OLT) for PON/FTTx

networks, and Ethernet switches for Active Ethernet connections. Modern MSANs often support all of these connections, as well as providing connections for additional circuits such as plain old telephone service (referred to as POTS) or Digital Signal 1 (DS1 or T1).

The defining function of a multiservice access node is to aggregate traffic from multiple subscribers. At the physical level, the MSAN also converts traffic from the *last mile technology* (for example, ADSL) to Ethernet for delivery to subscribers.

You can broadly categorize MSANs into three types based on how they forward traffic in the network:

- **Layer–2 MSAN**—This type of MSAN is essentially a Layer 2 switch (though typically not a fully functioning switch) with some relevant enhancements. These MSANs use Ethernet (or ATM) switching to forward traffic. The MSAN forwards all subscriber traffic upstream to an edge router that acts as the centralized control point and prevents direct subscriber-to-subscriber communication. Ethernet Link Aggregation (LAG) provides the resiliency in this type of network.

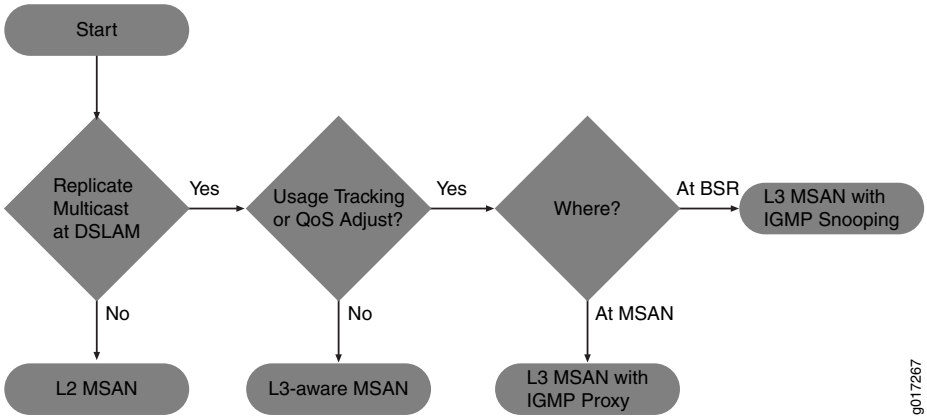
  Layer 2 DSLAMs cannot interpret IGMP, so they cannot selectively replicate IPTV channels.

- **Layer–3 aware MSAN**—This IP-aware MSAN can interpret and respond to IGMP requests by locally replicating a multicast stream and forwarding the stream to any subscriber requesting it. Layer 3 awareness is important when supporting IPTV traffic to perform channel changes (sometimes referred to as *channel zaps*). Static IP-aware MSANs always receive all multicast television channels. They do not have the ability to request that specific channels be forwarded to the DSLAM. Dynamic IP-aware DSLAMs, however, can inform the network to begin (or discontinue) sending individual channels to the DSLAM. Configuring IGMP proxy or IGMP snooping on the DSLAM accomplishes this function.

- **Layer–3 MSAN**—These MSANs use IP routing functionality rather than Layer 2 technologies to forward traffic. The advantage of this forwarding method is the ability to support multiple upstream links going to different upstream routers and improving network resiliency. However, to accomplish this level of resiliency, you must assign a separate IP subnetwork to each MSAN, adding a level of complexity that can be more difficult to maintain or manage.

In choosing a MSAN type, refer to Figure 2 on page 19:

Figure 2: Choosing an MSAN Type



Related Topics ■ Ethernet MSAN Aggregation Options on page 19

Ethernet MSAN Aggregation Options

Each MSAN can connect directly to an edge router (broadband services router or video services router), or an intermediate device (for example, an Ethernet switch) can aggregate MSAN traffic before being sent to the services router. Table 5 on page 19 lists the possible MSAN aggregation methods and under what conditions they are used.

Table 5: Ethernet MSAN Aggregation Methods

Method	When Used
Direct connection	Each MSAN connects directly to the broadband services router and optional video services router.
Ethernet aggregation switch connection	Each MSAN connects directly to an intermediate Ethernet switch. The switch, in turn, connects to the broadband services router or optional video services router.
Ethernet ring aggregation connection	Each MSAN connects to a ring topology of MSANs. The head-end MSAN (the device closest to the upstream edge router) connects to the broadband services router.

You can use different aggregation methods in different portions of the network. You can also create multiple layers of traffic aggregation within the network. For example, an MSAN can connect to a central office terminal (COT), which, in turn, connects to an Ethernet aggregation switch, or you can create multiple levels of Ethernet aggregation switches prior to connecting to the edge router.

Direct Connection

In the direct connection method, each MSAN has a point-to-point connection to the broadband services router. If an intermediate central office exists, traffic from multiple MSANs can be combined onto a single connection using wave-division multiplexing

(WDM). You can also connect the MSAN to a video services router. However, this connection method requires that you use a Layer 3 MSAN that has the ability to determine which link to use when forwarding traffic.

When using the direct connection method, keep the following in mind:

- We recommend this approach when possible to simplify network management.
- Because multiple MSANs are used to connect to the services router, and Layer 3 MSANs generally require a higher equipment cost, this method is rarely used in a multiedge subscriber management model.
- Direct connection is typically used when most MSAN links are utilized less than 33 percent and there is little value in combining traffic from multiple MSANs.

Ethernet Aggregation Switch Connection

An Ethernet aggregation switch aggregates traffic from multiple downstream MSANs into a single connection to the services router (broadband services router or optional video services router).

When using the Ethernet aggregation switch connection method, keep the following in mind:

- Ethernet aggregation is typically used when most MSAN links are utilized over 33 percent or to aggregate traffic from lower speed MSANs (for example, 1 Gbps) to a higher speed connection to the services router (for example, 10 Gbps).
- You can use an MX-series router as an Ethernet aggregation switch. For information about configuring the MX-series router in Layer 2 scenarios, see the *MX-series Layer 2 Configuration Guide* or the *MX-series Solutions Guide*.

Ring Aggregation Connection

In a ring topology, the remote MSAN that connects to subscribers is called the remote terminal (RT). This device can be located in the outside plant (OSP) or in a remote central office (CO). Traffic traverses the ring until it reaches the central office terminal (COT) at the head-end of the ring. The COT then connects directly to the services router (broadband services router or video services router).

NOTE: The RT and COT must support the same ring resiliency protocol.

You can use an MX-series router in an Ethernet ring aggregation topology. For information about configuring the MX-series router in Layer 2 scenarios, see the *MX-series Layer 2 Configuration Guide* or the *MX-series Solutions Guide*.

Related Topics

- Multiservice Access Node Overview on page 17

Chapter 4

Broadband Subscriber Management Solution Software Overview

Broadband Subscriber Management VLAN Architecture Overview

The subscriber management logical network architecture is as important as the physical network architecture. You configure the logical portion of the subscriber management network using virtual local area networks (VLANs).

Three VLAN models deliver multiple services to subscribers. These models include the following:

- **Service VLAN**—The service VLAN (S-VLAN) provides many-to-one (N:1) subscriber-to-service connectivity: The service VLAN carries a service (for example, data, video, or voice) to all subscribers instead of having different services share a VLAN. Adding a new service requires adding a new VLAN and allocating bandwidth to the new service. The service VLAN model enables different groups that are using the broadband network (for example, external application providers) to manage a given service. One limitation of service VLANs is the absence of any logical isolation between user sessions at the VLAN level. This lack of isolation requires that the multiservice access node (MSAN) and broadband services router provide the necessary security filtering.
- **Customer VLAN**—The customer VLAN (C-VLAN) provides one-to-one (1:1) subscriber-to-service connectivity: One VLAN carries all traffic to each subscriber on the network. Having a single VLAN per subscriber simplifies operations by providing a 1:1 mapping of technology (VLANs) to subscribers. You can also understand what applications any subscriber is using at any given time. Because you use only one VLAN to carry traffic to each subscriber, this approach is not affected when adding new services. However, using a pure C-VLAN model consumes more bandwidth because a single television channel being viewed by multiple subscribers is carried across the network several times—once on each

C-VLAN. This approach requires a more scalable, robust edge router that can support several thousand VLANs.

- **Hybrid C-VLAN**—The hybrid VLAN combines the best of both previous VLANs by using one VLAN per subscriber to carry unicast traffic and one shared multicast VLAN (M-VLAN) for carrying broadcast (multicast) television traffic. You can use both the *pure* and *hybrid* C-VLAN models in different portions of the network, depending upon available bandwidth and MSAN capabilities.

NOTE: The term *C-VLAN*, when used casually, often refers to a *hybrid* C-VLAN implementation.

We recommend using one of the C-VLAN models to simplify configuration and management when expanding services. However, some MSANs are limited to the number of VLANs they can support, limiting the ability to use either C-VLAN model.

NOTE: Most MSANs can support the service VLAN model.

Broadband Subscriber Management VLANs Across an MSAN

You configure VLANs to operate between the MSAN and the edge router (broadband services router or video services router). However, the MSAN might modify VLAN identifiers before forwarding information to the subscriber in the following ways:

NOTE: Not all MSANs support these options.

- The VLAN identifiers can be carried within the ATM VCs or they can be removed. The value of keeping the VLAN header is that it carries the IEEE 802.1p Ethernet priority bits. These priority bits can be added to upstream traffic by the residential gateway, allowing the DSLAM to easily identify and prioritize more important traffic (for example, control and VoIP traffic). Typically, a VLAN identifier of zero (0) is used for this purpose.
- In a C-VLAN model, the MSAN might modify the VLAN identifier so that the same VLAN is sent to each subscriber. This enables the use of the same digital subscriber line (DSL) modem and residential gateway configuration for all subscribers without the need to define a different VLAN for each device.

Customer VLANs and Ethernet Aggregation

The 12-bit VLAN identifier (VLAN ID) can support up to 4095 subscribers. When using an aggregation switch with a C-VLAN topology, and fewer than 4095 subscribers are connected to a single edge router port, the aggregation switch can transparently pass all VLANs. However, if the VLAN can exceed 4095 subscribers per broadband services router port, you must use VLAN stacking (IEEE 802.1ad, also known as Q-in-Q). VLAN stacking includes two VLAN tags—an outer tag to identify the destination MSAN and

an inner tag to identify the subscriber. For downstream traffic (that is, from the broadband services router or Ethernet switch to the MSAN), the outer tag determines which port to forward traffic. The forwarding device then uses the VLAN pop function on this tag before forwarding the traffic. The reverse process occurs for upstream traffic.

VLAN stacking is not necessary for S-VLANs or M-VLANs. However, for the hybrid (C-VLAN and M-VLAN) model, the Ethernet switch or services router must be able to pop or push tags onto C-VLAN traffic while not modifying M-VLAN packets.

VLANs and Residential Gateways

One function provided by a residential gateway is to enable each subscriber to have a private (in-home) network, unseen by other broadband subscribers, while enabling the subscriber to have multiple devices connected to the broadband network. This private network is made possible by using Network Address Translation (NAT).

Most conditional access systems require detecting the real IP address of the set-top box (STB). This security measure means that traffic to and from the STB must be bridged, not routed, across all network elements including aggregation switches, MSANs, and residential gateways. NAT cannot be used at the residential gateway for traffic to and from the STB. In addition, some residential gateways associate VLANs (or ATM virtual circuits) with ports. Traffic on a given VLAN is always forwarded to specific downstream port. Use caution when mapping VLANs on an MSAN.

Related Topics

- Static Subscriber Interfaces and VLAN Overview

Broadband Subscriber Management IGMP Model Overview

In an IPTV network, channel changes occur when a set-top box (STB) sends IGMP commands that inform an upstream device (for example, a multiservice access node [MSAN] or services router) whether to start or stop sending multicast groups to the subscriber. In addition, IGMP hosts periodically request notification from the STB about which channels (multicast groups) are being received.

You can implement IGMP in the subscriber management network in the following ways:

- **Static IGMP**—All multicast channels are sent to the MSAN. When the MSAN receives an IGMP request to start or stop sending a channel, it performs the request and then discards the IGMP packet.
- **IGMP Proxy**—Only multicast channels currently being viewed are sent to the MSAN. If the MSAN receives a request to view a channel that is not currently being forwarded to the MSAN, it forwards the request upstream. However, the upstream device does not see all channel change requests from each subscriber.
- **IGMP Snooping**—Only multicast channels currently being viewed are sent to the MSAN. The MSAN forwards all IGMP requests upstream, unaltered, even if it is already receiving the channel. The upstream device sees all channel change requests from each subscriber. Using IGMP snooping enables the broadband

services router to determine the bandwidth requirement of each multicast group and adjust the bandwidth made available to unicast traffic.

- **IGMP Passthrough**—The MSAN transparently passes IGMP packets upstream to the broadband services router.

IGMP hosts (sources) also periodically verify that they are sending the correct traffic by requesting that each client send information about what multicast groups it wants to receive. The responses to this *IGMP query* can result in a substantial upstream traffic burst.

IGMPv2 is the minimum level required to support IPTV, and is the most widely deployed. Emerging standards specify IGMPv3.

Related Topics
- Dynamic IGMP Configuration Overview

DHCP and Broadband Subscriber Management Overview

You use DHCP in broadband networks to provide IP address configuration and service provisioning. DHCP, historically a popular protocol in LANs, works well with Ethernet connectivity and is becoming increasingly popular in broadband networks as a simple, scalable solution for assigning IP addresses to subscriber home PCs, set-top boxes (STBs), and other devices.

The JUNOS broadband subscriber management solution currently supports the following DHCP allocation models:

- DHCP Local Server
- DHCP Relay

DHCP uses address assignment pools from which to allocate subscriber addresses. Address-assignment pools support both dynamic and static address assignment:

- Dynamic address assignment—A subscriber is automatically assigned an address from the address-assignment pool.
- Static address assignment—Addresses are reserved and always used by a particular subscriber.

NOTE: Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

Extended DHCP Local Server and Broadband Subscriber Management Overview

You can enable the services router to function as an extended DHCP local server. As an extended DHCP local server the services router, and not an external DHCP server, provides an IP address and other configuration information in response to a client request. The extended DHCP local server supports the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients.

Extended DHCP Relay and Broadband Subscriber Management Overview

You can configure extended DHCP relay options on the router and enable the router to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server. You can use DHCP relay in carrier edge applications such as video and IPTV to obtain configuration parameters, including an IP address, for your subscribers. The extended DHCP relay agent supports the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients.

Related Topics

- Extended DHCP Local Server Overview
- Extended DHCP Relay Agent Overview
- Address-Assignment Pools Overview

AAA Service Framework and Broadband Subscriber Management Overview

You use AAA Service Framework for all authentication, authorization, accounting, address assignment, and dynamic request services that the services router uses for network access. The framework supports authentication and authorization through external servers, such as RADIUS. The framework also supports accounting and dynamic-request CoA and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS.

NOTE: The broadband subscriber management solution currently supports the use of only RADIUS servers.

The broadband services router interacts with external servers to determine how individual subscribers access the broadband network. The router also obtains information from the external server for the following:

- Methods used for authentication and accounting.
- How accounting statistics are collected and used.
- How dynamic requests are handled.

Related Topics

- RADIUS Authentication and Accounting for Subscriber Access Management
- RADIUS-Initiated Change of Authorization (CoA) Overview
- RADIUS-Initiated Disconnect Overview

Class of Service and Broadband Subscriber Management Overview

Class of service (CoS) is a mechanism that enables you to divide traffic into classes and offer various levels of throughput and acceptable packet loss when congestion occurs. CoS also provides the option of using differentiated services when best-effort traffic delivery is insufficient. You can also configure the services router to provide

hierarchical scheduling for subscribers by dynamically adding or deleting queues when subscribers require services.

By using a dynamic profile, you can provide all subscribers in your network with default CoS parameters when they log in. For example, you can configure an access dynamic profile to specify that all subscribers receive a basic data service. If you use RADIUS variables in the dynamic profile, you can enable the service to be activated for those subscribers at login. You can also use variables to configure a service profile that enables subscribers to activate a service or upgrade to different services through RADIUS change-of-authorization (CoA) messages following initial login.

Related Topics
- CoS for Subscriber Access Overview

Policy and Control for Broadband Subscriber Management Overview

You can use the Juniper Networks Session and Resource Control (SRC) software to implement policy and control in the subscriber management network. The SRC software provides policy management, subscriber management, and network resource control functions that enable the creation and delivery of services across the network.

For additional information about the Juniper Networks SRC software, go to http://www.juniper.net/techpubs/software/management/src/.

Part 2

Configuring the Broadband Subscriber Management Solution

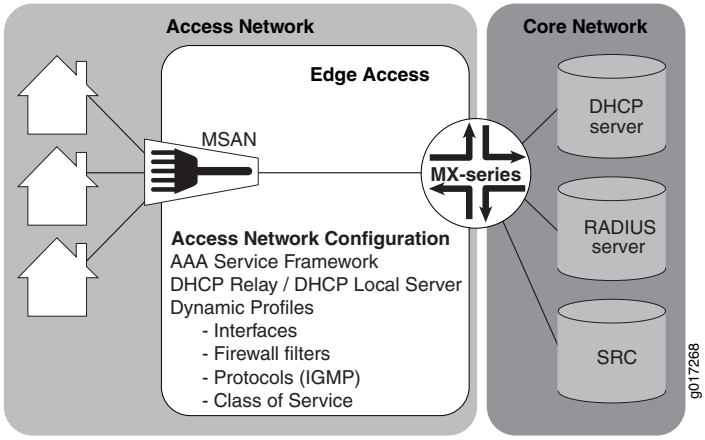
Chapter 5

Broadband Subscriber Management Configuration Overview

Broadband Subscriber Management Solution Topology and Configuration Elements

The network topology for the broadband subscriber management solution focuses on configuring the access network to which the MX-series routers connect. There are many possible broadband subscriber management configurations. Figure 3 on page 29 illustrates a basic topology model from which you can expand.

Figure 3: Basic Subscriber Management Solution Topology



When configuring the broadband subscriber management solution, specific configuration elements come into play. In one form or another, you must configure each of these elements for the subscriber management solution to function.

The configuration elements include the following:

- Subscriber network VLAN configuration
- AAA Service Framework configuration

- Addressing server or addressing server access configuration
- Dynamic profile configuration
- Core network configuration

Related Topics
- Triple Play Subscriber Management Network Topology Overview on page 31
- Configuring Top-Level Broadband Subscriber Management Elements on page 32

Subscriber Management Licensing

To enable some JUNOS subscriber management software features or router scaling levels, you must purchase, install, and manage certain software license packs. The presence on the router of the appropriate software license keys (passwords) determines whether you can configure and use certain features or configure a feature to a predetermined scale.

For information about how to purchase JUNOS software licenses, contact your Juniper Networks sales representative. For information about installing and managing software licenses that pertain to your broadband subscriber management network, see the *JUNOS Software Installation and Upgrade Guide*.

Related Topics
- Configuring Top-Level Broadband Subscriber Management Elements on page 32

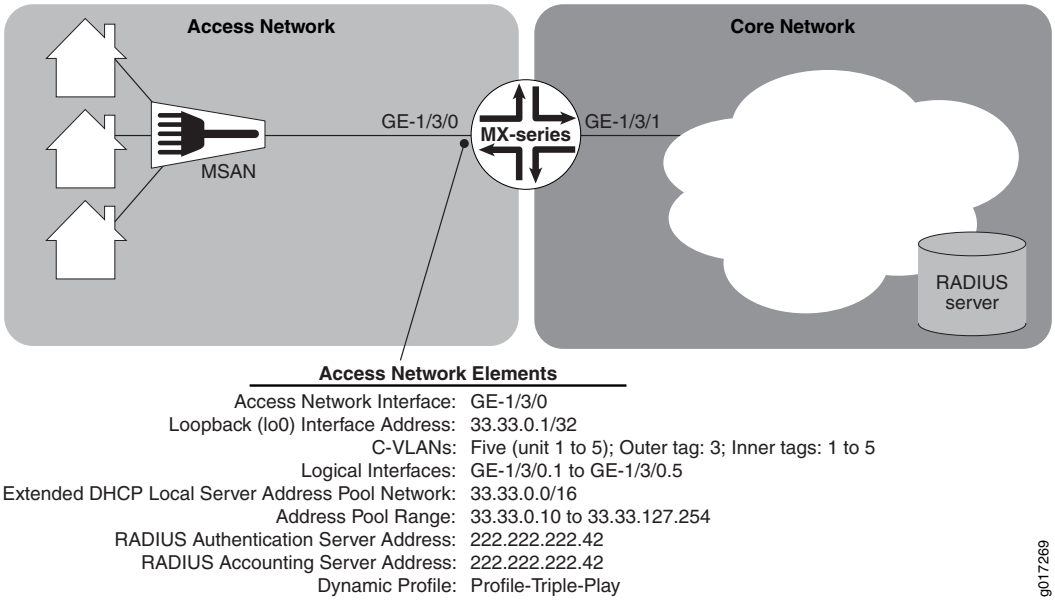
Chapter 6

Configuring a Basic Triple Play Subscriber Management Network

Triple Play Subscriber Management Network Topology Overview

This configuration explains the basics in configuring a basic triple-play (data, voice, and video) network. Figure 4 on page 32 provides the reference topology for this configuration example.

Figure 4: Triple Play Network Reference Topology



Related Topics ■ Configuring Top-Level Broadband Subscriber Management Elements on page 32

Configuring Top-Level Broadband Subscriber Management Elements

When configuring an MX-series router to act as a broadband services router (BSR) or video services router (VSR), you initially define elements that the router uses to define both subscriber access and the level of service a subscriber can have in your network. Many of these elements are profiles (groups of configuration statements) or static configuration components (like firewall filters) that typically do not change after you create them. After you define these elements, the router can use them to enable subscribers to gain access to your network.

The top-level steps for configuring the edge access in the subscriber management network include the following:

1. Configure the subscriber loopback interface and VLANs.

   See "Configuring Static Customer VLANs for the Broadband Subscriber Management Solution" on page 34.

2. Configure a class of service profile.

   See "Configuring a Global Class of Service Profile for the Subscriber Management Solution" on page 37.

3. Configure a firewall filter for use with the dynamic profile.

   See "Configuring Dynamic Firewall Filter Services for Use in Dynamic Profiles" on page 43.

4. Configure AAA Framework Services.

See “Configuring AAA Service Framework for the Broadband Subscriber Management Solution” on page 44.

5. Configure an address assignment pool for use by the address server.

   See “Configuring Address Server Elements for the Broadband Subscriber Management Solution” on page 46.

6. Configure DHCP local server to assign subscriber addresses.

   See “Configuring Address Server Elements for the Broadband Subscriber Management Solution” on page 46.

Related Topics

- Triple Play Subscriber Management Network Topology Overview on page 31
- Broadband Subscriber Management Solution Topology and Configuration Elements on page 29

Configuring a Loopback Interface for the Broadband Subscriber Management Solution

You must configure a loopback interface for use in the subscriber management access network. The loopback interface is automatically used for unnumbered interfaces.

NOTE: If you do not configure the loopback interface, the routing platform chooses the first interface to come online as the default. If you configure more than one address on the loopback interface, we recommend that you configure one to be the primary address to ensure that it is selected for use with unnumbered interfaces. By default, the primary address is used as the source address when packets originate from the interface.

To configure a loopback interface:

1. Edit the loopback interface.

   ```
   [edit]
   user@host#edit interfaces lo0
   ```

2. Edit the loopback interface unit.

   ```
   [edit interfaces lo0]
   user@host#edit unit 33
   ```

3. Edit the loopback interface family.

   ```
   [edit interfaces lo0 unit 33]
   user@host#edit family inet
   ```

4. Specify the loopback interface address.

   ```
   [edit interfaces lo0 unit 33]
   user@host#set address 33.33.0.1/32
   ```

Related Topics
- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- *JUNOS Network Interfaces Configuration Guide*

Configuring Static Customer VLANs for the Broadband Subscriber Management Solution

In this example configuration, the access interface (ge-1/3/0) connects to a device (that is, a DSLAM) on the access side of the network. You can define static customer VLANs (C-VLANs) for use by the access network subscribers.

To configure the customer VLANs:

1. Edit the access side interface.

   ```
   [edit]
   user@host#edit interfaces ge-1/3/0
   ```

2. Edit the interface unit for the first VLAN.

   ```
   [edit interfaces ge-1/3/0]
   user@host#edit unit 1
   ```

3. Define the VLAN tags for the first VLAN.

   ```
   [edit interfaces ge-1/3/0 unit 1]
   user@host#set vlan-tags outer 3 inner 1
   ```

4. Edit the family for the first VLAN.

   ```
   [edit interfaces ge-1/3/0 unit 1]
   user@host#edit family inet
   ```

5. Define the unnumbered address and the preferred source address for the first VLAN.

   ```
   [edit interfaces ge-1/3/0 unit 1 family inet]
   user@host#set unnumbered-address lo0.33 preferred-source-address 33.33.0.1
   ```

6. Repeat steps 2 through 5 for VLAN interface units 2 through 5.

Related Topics
- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- *JUNOS Network Interfaces Configuration Guide*

Configuring Dynamic Customer VLANs for the Broadband Subscriber Management Solution

In this example configuration, the access interface (ge-1/3/0) connects to a device (that is, a DSLAM) on the access side of the network. This procedure enables the dynamic creation of up to 5 customer VLANs (C-VLANs) for use by the access network subscribers.

To configure dynamic VLANs for the solution:

1. Configure a dynamic profile for dynamic VLAN creation.

   a. Name the profile.

      ```
      [edit]
      user@host# set dynamic-profiles VLAN-PROF
      ```

   b. Define the interface-name statement with the internal $junos-interface-ifd-name variable used by the router to match the interface name of the receiving interface.

      ```
      [edit dynamic-profiles VLAN-PROF]
      user@host# set interfaces $junos-interface-ifd-name
      ```

   c. Define the unit statement with the predefined $junos-interface-unit variable:

      ```
      [edit dynamic-profiles VLAN-PROF]
      user@host# set unit $junos-interface-unit
      ```

   d. (Optional) To configure the router to respond to any ARP request, specify the proxy-arp statement.

      ```
      [edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
         "$junos-interface-unit"]
      user@host# set proxy-arp
      ```

   e. Specify the VLAN ID variable.

      ```
      [edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
         "$junos-interface-unit"]
      user@host# set vlan-tags outer $junos-stacked-vlan-id
      ```

      The variable is dynamically replaced with an outer VLAN ID within the VLAN range specified at the [interfaces] hierarchy level.

   f. Specify the inner VLAN ID variable.

      ```
      [edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
         "$junos-interface-unit"]
      user@host# set vlan-tags inner $junos-vlan-id
      ```

      The variable is dynamically replaced with an inner VLAN ID within the VLAN range specified at the [interfaces] hierarchy level.

   g. Specify the family type.

      ```
      [edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
         "$junos-interface-unit"]
      user@host# set family inet
      ```

   h. (Optional) Enable IP and MAC address validation for dynamic IP demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
   "$junos-interface-unit" family inet]
user@host# set mac-validate strict
```

i. Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
   "$junos-interface-unit" family inet]
user@host# set unnumbered-address lo.0 preferred-source-address
   33.33.0.1
```

2. Associate the dynamic profile with the VLAN interface.

a. Access the interface that you want to use for creating VLANs.

```
[edit interfaces]
user@host# edit interfaces ge-1/3/0
```

b. Access the [auto-configure] hierarchy level.

```
[edit interfaces ge-1/3/0]
user@host# edit auto-configure
```

c. Access the [stacked-vlan-ranges] hierarchy level.

```
[edit interfaces ge-1/3/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

d. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-1/3/0 auto-configure stacked-vlan-ranges]
user@host# set dynamic-profile VLAN-PROF
```

3. Specify the Ethernet packet type that the VLAN dynamic profile can accept.

NOTE: This release supports only INET (IPv4) Ethernet packet types.

```
[edit interfaces ge-1/3/0 auto-configure stacked-vlan-ranges VLAN-PROF]
user@host# set accept inet
```

4. Define VLAN ranges for use by the dynamic profile when dynamically creating VLAN IDs. For this solution, specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. To mimic the static VLAN configuration, the following example specifies an outer stacked VLAN ID range of 3 and an inner stacked VLAN ID range of 1–5 (enabling a range from 1 through 5 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set ranges 3,1–5
```

Related Topics

- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- Broadband Subscriber Management VLAN Architecture Overview on page 21
- Dynamic 802.1Q VLAN Overview
- Configuring VLAN Dynamic Profiles
- Configuring VLAN Interfaces to Use Dynamic Profiles
- Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept
- Configuring VLAN Ranges for Use with Dynamic Profiles
- *JUNOS Network Interfaces Configuration Guide*

Configuring a Global Class of Service Profile for the Subscriber Management Solution

Configuring a Class of Service Profile

You can configure class of service (CoS) for all subscribers that successfully establish connection to the broadband network. After you create the CoS profile, you can attach it to subscriber interfaces using a dynamic profile.

Configuring a CoS profile includes the following general steps:

1. Configuring forwarding classes.
2. Configuring schedulers.
3. Configuring scheduler maps.
4. Configuring classifiers.
5. Configuring CoS interface properties.

In this configuration, we configure three forwarding classes, each with its own scheduler, and an IP precedence classifier for the traffic destined for the access network. Table 6 on page 37 provides an overview of the queue configuration:

Table 6: Class of Service Queue Configuration

Differentiated Services Classification	Bandwidth	Priority	Purpose
Expedited forwarding (EF)	128 Kbps	strict high	voice traffic

Table 6: Class of Service Queue Configuration *(continued)*

Differentiated Services Classification	Bandwidth	Priority	Purpose
Assured forwarding (AF)	29.4 Mbps	low	video traffic
Best effort (BE)	remainder	low	data traffic

Configuring CoS Fowarding Classes

Forwarding classes identify output queues for packets. For a classifier to assign an output queue to each packet, it must associate the packet with one of the following forwarding classes:

- Expedited forwarding (EF)—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- Assured forwarding (AF)—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with three drop probabilities: low, medium, and high.
- Best effort (BE)—Provides no service profile. For the BE forwarding class, loss priority is typically not carried in a class-of-service (CoS) value, and random early detection (RED) drop profiles are more aggressive.
- Network control (NC)—This class is typically high priority because it supports protocol control.

NOTE: The MX-series router enables you to configure up to eight forwarding class queues.

To configure forwarding class queues:

1. Edit the best effort queue.

   ```
   [edit]
   user@host#edit class-of-service forwarding-classes queue 0
   ```

2. Name the queue.

   ```
   [edit class-of-service forwarding-classes queue 0]
   user@host#set fc_be
   ```

3. Edit the expedited forwarding queue.

   ```
   [edit]
   user@host#edit class-of-service forwarding-classes queue 1
   ```

4. Name the queue.

   ```
   [edit class-of-service forwarding-classes queue 1]
   user@host#set fc_ef
   ```

5. Edit the assured forwarding queue.

```
[edit]
user@host#edit class-of-service forwarding-classes queue 2
```

6. Name the queue.

```
[edit class-of-service forwarding-classes queue 1]
user@host#set fc_ef
```

Configuring CoS Schedulers

CoS schedulers define the properties of output queues. These properties can include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue.

To configure CoS schedulers for the existing queues:

1. Create a scheduler and name it for the best effort traffic.

```
[edit]
user@host#edit class-of-service schedulers sched_be
```

2. Define the best effort scheduler buffer size.

```
[edit class-of-service schedulers sched_be]
user@host#set buffer-size remainder
```

3. Set the priority of the best effort scheduler.

```
[edit class-of-service schedulers sched_be]
user@host#set prioritiy low
```

4. Create a scheduler and name it for the expedited forwarding traffic.

```
[edit]
user@host#edit class-of-service schedulers sched_ef
```

5. Configure the transmit rate for the expedited forwarding scheduler.

```
[edit class-of-service schedulers sched_ef]
user@host#set transmit-rate 128k
```

6. Define the expedited forwarding scheduler buffer size.

```
[edit class-of-service schedulers sched_ef]
user@host#set buffer-size remainder
```

7. Set the priority of the expedited forwarding scheduler.

```
[edit class-of-service schedulers sched_ef]
user@host#set prioritiy strict-high
```

8. Create a scheduler and name it for the assured forwarding traffic.

```
[edit]
user@host#edit class-of-service schedulers sched_af
```

9. Configure the transmit rate for the assured forwarding scheduler.

```
[edit class-of-service schedulers sched_af]
user@host#set transmit-rate 29400000
```

10. Define the assured forwarding scheduler buffer size.

```
[edit class-of-service schedulers sched_af]
user@host#set buffer-size remainder
```

11. Set the priority of the expedited forwarding scheduler.

```
[edit class-of-service schedulers sched_af]
user@host#set prioritiy low
```

Configuring Scheduler Maps

After configuring both CoS forwarding classes and schedulers, you must use scheduler maps to associate them.

To map CoS forwarding classes to schedulers:

1. Create a forwarding map and name it.

```
[edit]
user@host#edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic
```

2. Edit the best effort forwarding class queue.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic]
user@host# edit forwarding-class fc_be
```

3. Associate the scheduler that you want this forwarding class to use.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic forwarding-c
   lass fc_be]
user@host#set scheduler sched_be
```

4. Edit the expedited forwarding class queue.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic]
user@host# edit forwarding-class fc_ef
```

5. Associate the scheduler that you want this forwarding class to use.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic forwarding-c
   lass fc_ef]
user@host#set scheduler sched_ef
```

6. Edit the assured forwarding class queue.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic]
user@host# edit forwarding-class fc_af
```

7. Associate the scheduler that you want this forwarding class to use.

```
[edit class-of-service scheduler-maps SchedulerMap_Triple_Play_Basic forwarding-c
   lass fc_af]
user@host#set scheduler sched_af
```

Configuring CoS Classifiers

You can override the default IP precedence classifier by defining a custom classifier. You can then apply the classifier to a logical interface.

To define a custom CoS classifier:

1. Create a Differentiated Services code point (DSCP) classifier and name it.

```
[edit]
user@host#edit class-of-service classifiers dscp Class_DSCP
```

NOTE: DSCP classifiers handle incoming IPv4 packets.

2. Edit the best effort forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP]
user@host#edit forwarding-class fc_be
```

3. Edit the loss priority level for the forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_be]
user@host#edit loss-priority high
```

4. Set code points for the loss priority level.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_be loss-p
   riority low]
user@host#set code-points be
```

5. Edit the expedited forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP]
user@host#edit forwarding-class fc_ef
```

6. Edit the loss priority level for the forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_ef]
user@host#edit loss-priority low
```

7. Set code points for the loss priority level.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_ef loss-p
   riority low]
user@host#set code-points ef
```

8. Edit the assured forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP]
user@host#edit forwarding-class fc_af
```

9. Edit the loss priority level for the forwarding class queue.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_af]
user@host#edit loss-priority low
```

10. Set code points for the loss priority level.

```
[edit class-of-service classifiers dscp Class_DSCP forwarding-class fc_af loss-p
  riority low]
user@host#set code-points af41
```

Configuring CoS Interface Properties

Configuring CoS interface properties enables the router to throttle and classify the traffic from the Internet that is sent to subscriber local loops. Limiting the traffic to the access network ensures that the traffic sent to the subscriber local loops does not exceed the current data transmission rate of those lines. Limiting traffic also ensures that changes to subscriber local loop speeds do not cause bandwidth contention at the subscriber's residential gateway. You apply the classifier to the core-facing interface to classify incoming traffic for the queues you are using in the access network.

To configure CoS interfaces:

1. Edit the core CoS interface you want to configure.

```
[edit]
user@host#edit class-of-service interfaces ge-1/3/0
```

2. Edit the interface shaping rate.

```
[edit class-of-service interfaces ge-1/3/0]
user@host#edit class-of-service interfaces ge-1/3/0 shaping-rate
```

3. Set the shaping rate value to throttle traffic to the subscriber local loops.

```
[edit class-of-service interfaces ge-1/3/0 shaping-rate]
user@host#set 500m
```

4. Edit the interface connected to the core network.

```
[edit]
user@host#edit class-of-service interfaces ge-1/3/1
```

5. Edit the interface unit.

```
[edit class-of-service interfaces ge-1/3/1]
user@host#edit unit 0
```

6. Edit the interface unit classifiers.

```
[edit class-of-service interfaces ge-1/3/1 unit 0]
```

```
user@host#edit classifiers
```

7. Apply the classifier to the interface to classify traffic coming from the Internet.

```
[edit class-of-service interfaces ge-1/3/1 unit 0 classifiers]
user@host#set dscp Class_DSCP
```

Configuring Dynamic Firewall Filter Services for Use in Dynamic Profiles

Firewall filters provide rules that define whether to permit or deny packets that are transiting an interface on a router. You can configure firewall filters for use in dynamic profiles. After you configure dynamic firewall filters, you can specify which filters you want to apply to subscriber interfaces using a dynamic profile.

To create a firewall filter:

1. Create and name a firewall filter.

```
[edit]
user@host#edit firewall filter fw_fltr_af41
```

2. Specify the filter to be interface specific.

```
[edit firewall filter fw_fltr_af41]
user@host#set interface-specific
```

3. Edit a first term for the firewall filter.

```
[edit firewall filter fw_fltr_af41]
user@host#edit firewall filter fw_fltr_af41 term 1
```

4. Set the from match condition.

```
[edit firewall filter fw_fltr_af41 term 1]
user@host#set from dscp af41
```

5. Set the then action to take when a match occurs.

```
[edit firewall filter fw_fltr_af41 term 1]
user@host#then count c2 accept
```

6. Edit a second term for the firewall filter.

```
[edit firewall filter fw_fltr_af41]
user@host#edit firewall filter fw_fltr_af41 term 2
```

7. Set the then action to take when a match occurs for term 1.

```
[edit firewall filter fw_fltr_af41 term 1]
user@host#then accept
```

8. Apply the dynamic firewall filter to interfaces using a dynamic profile.

See “Configuring a Dynamic Profile for the Triple Play Solution” on page 48.

Related Topics

- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- Dynamic Firewall Filters Overview
- Dynamic Profiles Overview
- *JUNOS Policy Framework Configuration Guide*

Configuring AAA Service Framework for the Broadband Subscriber Management Solution

Configuring RADIUS Server Access Information

Define the RADIUS server address and secret data that RADIUS access profiles can reference. Define an access profile that includes specific RADIUS configuration.

To configure RADIUS server access:

1. Edit router access to the RADIUS server.

   ```
   [edit]
   user@host#edit access radius-server
   ```

2. Set the address to the RADIUS server.

   ```
   [edit access radius-server]
   user@host#set 222.222.222.42
   ```

3. Edit the RADIUS server.

   ```
   [edit access radius-server]
   user@host#edit 222.222.222.42
   ```

4. Configure the source address for the RADIUS server.

   ```
   [edit access radius-server 222.222.222.42]
   user@host#set source-address 222.222.222.1
   ```

5. Configure the secret for the RADIUS server.

   ```
   [edit access radius-server 222.222.222.42]
   user@host#set secret "$EcReTRad1uSdAta4f0rTh3rtR"
   ```

Configuring RADIUS Server Access Profile

You can define a RADIUS access profile that references defined RADIUS servers and includes specific RADIUS configuration for authentication and accounting.

To configure a RADIUS access profile:

1. Create and name a RADIUS access profile.

   ```
   [edit]
   user@host#edit access profile AccessProfile_general
   ```

2. Edit the order in which authentication mechanisms are used.

   ```
   [edit access profile AccessProfile_general]
   user@host#set authentication-order radius
   ```

3. Edit the RADIUS access addresses.

   ```
   [edit access profile AccessProfile_general]
   user@host#edit access profile AccessProfile_general radius
   ```

4. Set the address or address list for the RADIUS authentication server.

   ```
   [edit access profile AccessProfile_general radius]
   user@host#set authentication-server 222.222.222.42
   ```

5. Set the address or address list for the RADIUS accounting server.

   ```
   [edit access profile AccessProfile_general radius]
   user@host#set accounting-server 222.222.222.42
   ```

6. Edit the RADIUS accounting values for the access profile.

   ```
   [edit access profile AccessProfile_general]
   user@host#edit accounting
   ```

7. Set the RADIUS accounting order.

   ```
   [edit access profile AccessProfile_general accounting]
   user@host#set order radius
   ```

8. Specify that RADIUS accounting stop when a user fails authentication but is granted access.

   ```
   [edit access profile AccessProfile_general accounting]
   user@host#set accounting-stop-on-failure
   ```

9. Specify that RADIUS accounting stop when access is denied to a subscriber.

   ```
   [edit access profile AccessProfile_general accounting]
   user@host#set accounting-stop-on-access-deny
   ```

10. Specify that RADIUS provide immediate updates.

    ```
    [edit access profile AccessProfile_general accounting]
    user@host#set immediate-update
    ```

11. Specify the amount of time (in minutes) between RADIUS updates.

    ```
    [edit access profile AccessProfile_general accounting]
    user@host#set update-interval 10
    ```

12. Specify that RADIUS accounting report only subscriber uptime.

```
[edit access profile AccessProfile_general accounting]
user@host#set statistics time
```

Related Topics
- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- AAA Service Framework Overview

Configuring Address Server Elements for the Broadband Subscriber Management Solution

Configuring an Address Assignment Pool

Address assignment pools enable you to specify groups of IP addresses that different client applications can share. In this configuration, the extended DHCP local server configuration uses the address pool to provide addresses to subscribers that are accessing the network.

To configure an address assignment pool:

1. Create and name an address assignment pool.

```
[edit]
user@host#edit access address-assignment pool AddressPool_1
```

2. Edit the address pool family.

```
[edit access address-assignment pool AddressPool_1]
user@host#edit family inet
```

3. Define the address pool network.

```
[edit access address-assignment pool AddressPool_1 family inet]
user@host#set network 33.33.0.0/16
```

4. Specify the network for the pool.

```
[edit access address-assignment pool AddressPool_1 family inet]
user@host#set network 33.33.0.0/16
```

5. Set the address range for the network.

```
[edit access address-assignment pool AddressPool_1 family inet]
user@host#set range all low 33.33.0.10 high 33.33.127.254
```

6. Edit the family DHCP attributes.

```
[edit access address-assignment pool AddressPool_1 family inet]
user@host#edit family inet dhcp-attributes
```

7. Set the maximum lease time.

   ```
   [edit access address-assignment pool AddressPool_1 family inet dhcp-attributes]
   user@host#set maximum-lease-time 3600
   ```

8. Set the grace period.

   ```
   [edit access address-assignment pool AddressPool_1 family inet dhcp-attributes]
   user@host#set grace–periord 60
   ```

9. Set the router IP address that you want advertised to subscribers.

   ```
   [edit access address-assignment pool AddressPool_1 family inet dhcp-attributes]
   user@host#set router 33.33.0.1
   ```

10. Specify which access profile you want to instantiate.

    ```
    [edit]
    user@host#set access-profile AccessProfile_general
    ```

Configuring Extended DHCP Local Server

You can enable the MX-series router to function as an extended DHCP local server. The extended DHCP local server provides IP addresses and other configuration information to a subscriber logging into the network.

To configure the DHCP local server:

1. Edit the routing system services.

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

2. Edit the DHCP local server.

   ```
   [edit system services]
   user@host#edit dhcp-local-server
   ```

3. Edit the DHCP local server trace options.

   ```
   [edit system services dhcp-local-server]
   user@host#edit traceoptions
   ```

4. Specify a log file into which you want trace option information to be saved.

   ```
   [edit system services dhcp-local-server traceoptions]
   user@host#set file dhcp-server-msgs.log
   ```

5. Specify the DHCP local server message operations that you want saved in the log file.

   ```
   [edit system services dhcp-local-server traceoptions]
   user@host#set flag all
   ```

6. Define the DHCP pool match order.

```
[edit system services dhcp-local-server]
user@host#set pool-match-order ip-address-first
```

7. Set the authentication password.

```
[edit system services dhcp-local-server]
user@host#set authentication password auth-psswrd
```

8. Edit the values you want included with the username.

```
[edit system services dhcp-local-server]
user@host#edit authentication username-include
```

9. Set the values you want included with the username.

```
[edit system services dhcp-local-server username-include]
user@host#set domain-name yourcompany.com
user@host#set user-prefix user-defined-prefix
```

10. Create and name a DHCP local server group.

```
[edit system services dhcp-local-server]
user@host#edit group dhcp-ls-group
```

11. Specify a dynamic profile that you want the DHCP local server group to use.

```
[edit system services dhcp-local-server group dhcp-ls-group]
user@host#set dynamic-profile Profile-Triple_Play
```

12. Assign interfaces to the group.

```
[edit system services dhcp-local-server group dhcp-ls-group]
user@host# set interface ge-1/3/0.1 upto ge-1/3/0.5
```

Related Topics

- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- Address-Assignment Pools Overview
- Extended DHCP Local Server Overview

Configuring a Dynamic Profile for the Triple Play Solution

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide dynamic subscriber access and services for broadband applications. These services are assigned dynamically to interfaces.

To configure a dynamic profile:

1. Create and name the dynamic profile.

```
[edit]
user@host#edit dynamic-profiles Profile-Triple_Play
```

2. Edit the profile dynamic interfaces.

```
[edit dynamic-profiles Profile-Triple_Play]
user@host#edit interfaces
```

3. Set the dynamic interfaces and unit variables.

```
[edit dynamic-profiles Profile-Triple_Play interfaces]
user@host#set $junos-interface-ifd-name unit $junos-underlying-interface-unit
```

4. Edit dynamic interfaces.

```
[edit dynamic-profiles Profile-Triple_Play interfaces]
user@host#edit dynamic-profiles Profile-Triple_Play interfaces
   $junos-interface-ifd-name unit $junos-underlying-interface-unit
```

5. Set the dynamic interface family.

```
[edit dynamic-profiles Profile-Triple_Play interfaces "$junos-interface-ifd-name"
   unit "$junos-underlying-interface-unit"]
user@host#set family inet
```

6. Edit the dynamic interface family.

```
[edit dynamic-profiles Profile-Triple_Play interfaces "$junos-interface-ifd-name"
   unit "$junos-underlying-interface-unit"]
user@host#edit family inet
```

7. Specify the input filter that you want to apply to each dynamic interface when it is created.

```
[edit dynamic-profiles Profile-Triple_Play interfaces "$junos-interface-ifd-name"
   unit "$junos-underlying-interface-unit" family inet]
user@host#set filter input fltr_af41
```

8. Specify the output filter that you want to apply to each dynamic interface when it is created.

```
[edit dynamic-profiles Profile-Triple_Play interfaces "$junos-interface-ifd-name"
   unit "$junos-underlying-interface-unit" family inet]
user@host#set filter output fltr_af41
```

9. Edit dynamic class of service.

```
[edit dynamic-profiles Profile-Triple_Play]
user@host#edit class-of-service
```

10. Edit the dynamic CoS traffic control profile.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service]
user@host#edit traffic-control-profiles
```

11. Create and name a traffic control profile.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service traffic-control-profiles]
user@host#edit TrafficProfile_Triple_Play
```

12. Specify a scheduler map that you want the dynamic CoS traffic control profile to use.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service traffic-control-profile]
user@host#set scheduler-map SchedulerMap_Triple_Play_Basic
```

13. Specify the shaping rate that you want the dynamic CoS traffic control profile to use.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service traffic-control-profile]
user@host#set shaping-rate 32700000
```

14. Edit the dynamic CoS interfaces.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service]
user@host#edit interfaces
```

15. Apply CoS to the dynamic interfaces and apply an output traffic control profile.

```
[edit dynamic-profiles Profile-Triple_Play class-of-service]
user@host#set interfaces $junos-interface-ifd-name unit
   $junos-underlying-interface-unit output-traffic-control-profile otcp-profile
```

Related Topics

- Configuring Top-Level Broadband Subscriber Management Elements on page 32
- Dynamic Profiles Overview

Part 3
Monitoring the Broadband Subscriber Management Solution

Chapter 7

Related Broadband Subscriber Management CLI Commands

You can use a number of JUNOS CLI commands to monitor and troubleshoot a configured subscriber management solution. The following sections provide links to CLI commands that are related to the subscriber management configuration and where to locate details about each command.

Subscriber Management AAA and DHCP CLI Commands

Table 7 on page 53 provides a list of AAA–related and DHCP–related CLI commands that are associated with subscriber management configuration. These commands appear in the *JUNOS System Basics and Services Command Reference*.

Table 7: Subscriber Management AAA and Address Assignment Pools CLI Commands

CLI Command	Purpose
show network-access aaa statistics	Display AAA accounting and authentication statistics.
show network-access aaa subscribers	Display subscriber-specific AAA statistics.
show network-access address-assignment pool	Display state information for each address-assignment pool.

Subscriber Management DHCP Local Server CLI Commands

Table 8 on page 54 provides a list of DHCP local server–related CLI commands that are associated with subscriber management configuration. These commands appear in the *JUNOS System Basics and Services Command Reference*.

Table 8: Subscriber Management DHCP Local Server CLI Commands

CLI Command	Purpose
show dhcp server binding	Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (DHCP) local server.
show dhcp server statistics	Display extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
clear dhcp server binding	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the extended DHCP local server.
clear dhcp server statistics	Clear all extended Dynamic Host Configuration Protocol (DHCP) local server statistics.

Subscriber Management DHCP Relay CLI Commands

Table 9 on page 54 provides a list of DHCP relay–related CLI commands that are associated with subscriber management configuration. These commands appear in the *JUNOS Routing Protocols and Policies Command Reference*.

Table 9: Subscriber Management DHCP Relay CLI Commands

CLI Command	Purpose
show dhcp relay binding	Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.
show dhcp relay statistics	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
clear dhcp relay binding	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.
clear dhcp relay statistics	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

Subscriber Management Interface CLI Commands

Table 10 on page 54 provides a list of interface–related CLI commands that are associated with subscriber management configuration. These commands appear in the *JUNOS Interfaces Command Reference*.

Table 10: Subscriber Management Interface CLI Commands

CLI Command	Purpose
show interfaces (Loopback)	Display information about configured loopback interfaces.

Table 10: Subscriber Management Interface CLI Commands *(continued)*

CLI Command	Purpose
show interfaces (Aggregated Ethernet) show interfaces (Fast Ethernet) show interfaces (Gigabit Ethernet)	Display information about configured interfaces. This command includes brief, detail, and extensive options that you can use to view all interfaces or a specific Ethernet or LAG interface.
show interfaces demux0 (Demux Interfaces)	Display information about configured Demux interfaces.
show interfaces filters	Display all firewall filters that are installed on each interface.
show interfaces routing	Have the routing protocol process display its view of the state of the router's interfaces.

Subscriber Management Dynamic Protocol CLI Commands

Table 11 on page 55 provides a list of dynamic protocol–related CLI commands that are associated with subscriber management configuration. These commands appear in the *JUNOS Routing Protocols and Policies Command Reference*.

Table 11: Subscriber Management Dynamic Protocol CLI Commands

CLI Command	Purpose
show igmp interface	Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.
show igmp statistics	Display Internet Group Management Protocol (IGMP) statistics.

Subscriber Management Subscriber CLI Commands

Table 12 on page 55 provides the subscriber–related CLI command that is associated with subscriber management configuration. This command appears in the *JUNOS System Basics and Services Command Reference*.

Table 12: Subscriber Management Subscriber CLI Commands

CLI Command	Purpose
show subscribers	Display information for active subscribers.

Part 4
Index

Index

E

F

G

H

I

L

M

N

P

R

S

T

V