JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

Service Manager

Release
14.1.x

Published: 2012-12-20

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

JunosE™ Software for E Series™ Broadband Services Routers Service Manager
Release 14.1.x

Revision History
December 2012—FRS JunosE 14.1.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

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

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

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

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

Table 1: Notice Icons

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

Table 2 on page xiv defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

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

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

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

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

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

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. 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 or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

How Service Manager Works

Service Manager Overview

The JunosE Service Manager application provides authentication, service selection, and service activation and deactivation to subscribers. The application also collects accounting information and statistics, and monitors subscriber and service sessions.

Service Manager supports two client types—RADIUS and CLI. Service Manager starts when it receives a request from a RADIUS or CLI client. For RADIUS clients, RADIUS Access-Accept messages and Change-of-Authorization-Request (CoA-Request) messages can create and delete Service Manager subscriber sessions and activate and deactivate service sessions. For CLI clients, CLI commands create and delete the subscriber sessions and activate and deactivate service sessions.

A subscriber's service is based on a service definition — service definitions can include profiles, policies, and quality of service (QoS) settings that define the scope of a service granted to the subscriber. Service definitions can also specify statistics configurations.

Service Manager provides convenience and flexibility to both service providers and subscribers.

- Providers are able to separate services and access technology and also to eliminate unprofitable flat-rate billing. They gain the ability to efficiently design, manage, and deliver services that subscribers want, and then bill subscribers based on connect time, bandwidth, and the actual service used.
- Subscribers benefit by gaining access to multiple simultaneous services—subscribers can dynamically connect to and disconnect from the services, when they want and for how long they want. They are billed based on the service type and usage, rather than being charged a set rate regardless of usage.

Related Documentation

- Service Manager Platform Considerations on page 4
- Service Definitions Overview on page 9

- Configuring the Service Manager License on page 39
- Configuring Service Manager

Service Manager Performance Considerations

Like any application, Service Manager requires a certain amount of system resources. Consider the following guidelines to maximize the performance of Service Manager when delivering subscriber services:

- Minimize service definitions—Use the minimum number of JunosE commands in a service definition to specify a service.
- Reference objects in service definitions—Referencing commonly used objects is more resource-efficient than using unique objects for each subscriber (for example, using a subscriber's IP address as a match criteria in a classifier list).
- Preprovision frequently used services— Preprovisioning saves resources by requiring Service Manager to build a popular service only once. You then reuse the original service when you activate future subscriber service sessions. See "Preprovisioning Service Sessions" on page 53 for details.
- Capture volume statistics when needed—Repeatedly capturing volume statistics can waste resources.

Related Documentation

- Service Definitions Overview on page 9
- Overview of Referencing Policies in Service Definitions on page 8
- Creating Service Definitions on page 41
- Service Session Profiles Overview on page 29
- Preprovisioning Service Sessions on page 53

Service Manager Platform Considerations

Service Manager is supported on all E Series routers. For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Related Documentation

- Service Manager Overview on page 3
- Service Manager References on page 5
- Configuring the Service Manager License on page 39

Service Manager References

For more information about the topics covered in this chapter, see the following documents:

- Data-Over-Cable Service Interface Specifications (DOCSIS) 2.0 Radio Frequency Interface Specification CM-SP-RFIv2.0-I10-051209.
- For information about using the JunosE Software's macro language, see the *Writing CLI Macros* chapter in *JunosE System Basics Configuration Guide*.
- For information about setting up policy-based routing features for Service Manager, such as rate-limit profiles, classifier control lists, policy lists, and hierarchical and merged policies, see the *JunosE Policy Management Configuration Guide*.
- For information about creating QoS profiles and QoS parameters, see the *JunosE Quality of Service Configuration Guide*.
- For information about creating IPv4 interface profiles, see the *Configuring IP* chapter in *JunosE IP, IPv6, and IGP Configuration Guide*.

Related Documentation

- Service Manager Overview on page 3
- Service Manager Terms and Acronyms
- Service Manager Platform Considerations on page 4
- Service Definitions Overview on page 9
- Configuring Service Manager

CHAPTER 2

Service Definitions for QoS Policies and Profiles

QoS for Service Manager Considerations

When you specify QoS configurations in Service Manager, the following considerations apply.

RADIUS or Service Manager

We recommend that you choose either RADIUS or Service Manager to create a single parameter instance. If you use both RADIUS and Service Manager, parameter instances activated using Service Manager take precedence.

Interoperability with Other Service Components

Service Manager removes QoS profiles and parameter instances if other components in the service definition (for example, policies) cause an error.

QoS Statistics

Service Manager counts references of parameter instances in profiles. The reference count is incremented each time the parameter is configured through the CLI, RADIUS, or Service Manager. The reference count is decremented each time the parameter is unconfigured, such as through service deactivation. Modifications to parameter instances are also reference counted, using a separate reference count. Parameter instances are removed when both reference counts reach zero.

Service Manager also counts references of modified parameters in profiles using the **add** keyword. The reference count is incremented each time the parameter is modified though service activation with the **add** keyword. The reference count is decremented each time the parameter is modified through service deactivation. References of regular parameter instances are also counted, using a separate reference count. Parameter instances are removed when both reference counts reach zero.

Ranges

You can verify ranges for parameter instances by specifying a range in the parameter definition using the **range** command.

When activating the service or modifying parameters, Service Manager verifies the value of the parameter instance to be within the specified range and generates an informational log message indicating the value is outside the range. Service Manager does not verify ranges when you specify the parameter instances within profiles at the time of configuration.

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Specifying QoS Profiles in Service Definitions on page 78
- Referencing QoS Configurations in Service Definitions on page 77
- Modifying QoS Configurations with Service Manager on page 81
- Removing QoS Configurations Referenced by Service Manager on page 84

Overview of Referencing Policies in Service Definitions

In Profile Configuration mode, policy interface commands for IP and L2TP allow attachments to be merged into any existing merge-capable attachment at an attachment point. Merged policies are dynamically created. Service Manager can request that multiple interface profiles be applied or removed at an interface as part of service activation or deactivation. Service Manager also specifies whether or not the attachments created from these interface profiles persist on subsequent reloads.

Service Manager can specify whether a component policy attachment is non-volatile. If the interface where the component policy is attached is volatile, then policy management makes the attachment volatile even when the Service Manager specifies otherwise. A non-volatile interface can have both volatile and non-volatile component policy attachments. The merged policy that is created is the merge of all component policies attached at a given attachment point regardless of their volatility. The merged policy and its attachments are always volatile and reconstructed on each reload operation.

For further details on merging policies, see the *Merging Policies* chapter in *JunosE Policy Management Configuration Guide*.

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Referencing QoS Configurations in Service Definitions on page 77
- Modifying QoS Configurations with Service Manager on page 81
- Removing QoS Configurations Referenced by Service Manager on page 84
- Specifying QoS Profiles in Service Definitions on page 78

Service Definitions Overview

A service definition is a high-level, platform-independent template that defines a service that you want to let your subscribers use. You use the JunosE Software's embedded macro language on your computer to create the macro file that defines the service. You copy and install the macro file on the E Series Broadband Services Routers, and then you can associate the service definition with subscribers to create their service sessions.

Service definitions gives you flexibility by enabling you to use:

- A single service definition to create a service for multiple subscribers.
- Parameterized service definitions to create variations of a service definition.
- Different service definitions to create multiple services for a single subscriber.

A service definition might use the following types of JunosE objects to define the characteristics and capabilities of the service you want to provide:

- Interface profiles—Specify a set of characteristics that can be dynamically assigned to IP interfaces. A service definition must use at least one interface profile.
- Policy lists—Specify policy actions for traffic traversing an interface.
- Classifier lists—Specify the criteria by which the router defines a packet flow.
- Rate-limit profiles—Specify a set of bandwidth attributes and associated actions that limit a classified packet flow or a source interface to a rate that is less than the physical rate of the port.
- QoS parameters—Specify attributes such as shaping rate, shared-shaping rate, assured rate, and scheduler weight for scheduler nodes and queues.
- QoS profiles—Specify queue, drop statistics gathering, and scheduler configuration for an interface hierarchy.

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Overview of Referencing Policies in Service Definitions on page 8
- Referencing QoS Configurations in Service Definitions on page 77
- Specifying QoS Profiles in Service Definitions on page 78

CHAPTER 3

How Service Sessions Work

Overview of Managing and Activating Service Sessions

You can use either RADIUS or the CLI to manage, activate, and deactivate service sessions. The following list describes some of the differences between using RADIUS and the CLI to manage the Service Manager application.

- RADIUS-based login and RADIUS CoA support:
  - Provides dynamic activation and deactivation based on subscriber service selection
  - Provides greater flexibility and efficient management for a large number of subscribers and services
  - Enables you to use mutual exclusion (mutex) groups to create mutex services (RADIUS CoA only)
- CLI-based support:
  - Provides static activation and deactivation for subscribers who are always logged in
  - Is useful for testing new service definitions
  - Enables you to preprovision services that you can activate later

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Overview of Managing Subscriber Service Sessions Using the CLI on page 13

Overview of Managing Subscriber Service Sessions Using RADIUS

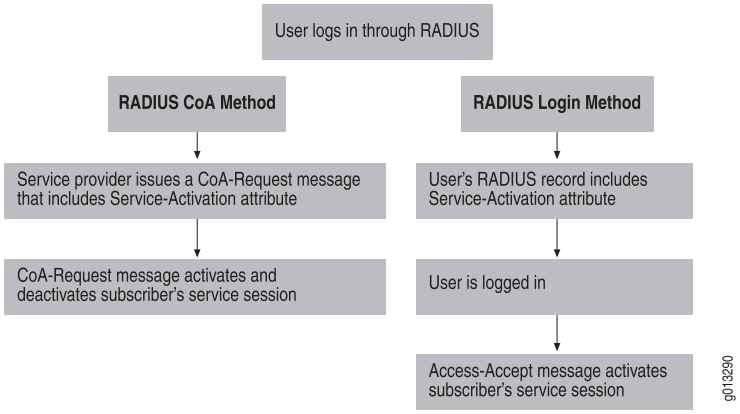
Service Manager supports two RADIUS-based methods for dynamically activating subscriber service sessions. Dynamic service sessions that RADIUS activates are not stored in NVS. Both methods can also apply optional statistics and session threshold (volume and time) configurations. The two methods differ in how Service Manager activates a subscriber service session:

- RADIUS login method—The service session is activated when the subscriber logs in. At login, RADIUS verifies that the Activate-Service attribute is configured in the subscriber's RADIUS record. RADIUS then uses vendor-specific attributes (VSAs) in the Access-Accept packet to activate the service session for the subscriber. This method is useful when your subscribers are not currently logged in.
- RADIUS CoA method—Supports dynamic service selection for subscribers. For example, the subscriber might have logged in without a service, or might have used the RADIUS login method to activate a service at login. If no service was activated at login (because of no Activate-Service attribute in the user's RADIUS record), you can later use the CoA method and a separate RADIUS record to create a subscriber session and activate a service session for the subscriber. Or, if the RADIUS login method was used and the subscriber already has an active service session, you can use the CoA method and a new RADIUS record to activate a new service session for the subscriber (and optionally deactivate the existing service session). The RADIUS CoA method is useful when you have a large number of users already logged in through RADIUS and you want to activate new services for them. This method is also used for the guided entrance service described in "Example: Guided Entrance Service Definition" on page 101.

  The RADIUS CoA method also supports the use of mutex groups to create mutex services. See "Overview of Activating and Deactivating Subscriber Services Using Mutex Groups" on page 19.

Figure 1 on page 13 compares the two RADIUS-based methods.

Figure 1: Comparing RADIUS Login and RADIUS CoA Methods



Related Documentation

- Service Session Profiles Overview on page 29
- Overview of Managing and Activating Service Sessions on page 11
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48
- Overview of Activating and Deactivating Subscriber Services Using Mutex Groups on page 19

Overview of Managing Subscriber Service Sessions Using the CLI

The CLI-based Service Manager creates static subscriber sessions and service sessions. You can also use CLI commands to immediately deactivate subscriber service sessions. The CLI-based support is particularly useful for:

- Testing your service definitions—for example, you might use the CLI commands to verify that a newly created service definition is correct. When you are satisfied with the service definition, you can then use RADIUS to activate the service for your subscribers.
- Preprovisioning Service Manager services—preprovisioning improves performance and efficiency by freeing Service Manager from having to repeatedly create and remove a service that you activate and deactivate for multiple subscribers. See "Preprovisioning Service Sessions" on page 53 for more information about service preprovisioning.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Overview of Managing and Activating Service Sessions on page 11
- Overview of Activating Subscriber Service Sessions Using the CLI on page 14
- Activating Subscriber Sessions Using the CLI on page 51
- Preprovisioning Service Sessions on page 53
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18

Overview of Activating Subscriber Service Sessions Using the CLI

A subscriber session represents a specific subscriber—the session consists of the subscriber's name, the interface used for the session, and any active services for the subscriber. A subscriber can have one subscriber session active at any given time.

You create a subscriber's service session when you assign a service definition to a subscriber session. Like an AAA-created service, a single subscriber session can have multiple simultaneous service sessions. You can use one method to create the subscriber session, and then a different method to activate the subscriber's service session. For example, you might use RADIUS to create the AAA subscriber session, then use the CLI to activate the service session for the subscriber, You can optionally specify a service session profile that you want to attach to the service session.

You can use the CLI to activate a service session based on subscriber information or owner information:

- Subscriber name and interface method—Activates the service session based on the subscriber name and the interface that the subscriber is using for this subscriber session.
- Owner name and ID method—Activates the service session based on the owner that created the subscriber session and the ID that was generated by the owner. For example, if RADIUS is used to create the subscriber session, the owner name is AAA and the owner ID is the Acct-Session-ID that was generated by RADIUS during subscriber creation.

NOTE: You must specify the parameter values in the order in which the parameters appear in the template name of the service definition file. Enclose the service definition name in double quotation marks, with the service's parameter values in parentheses. For example, for the tiered service that is defined in "Creating Service Definitions" on page 41, the template name is:

```
<# tiered(inputBW, outputBW) #>
```

Use the following format with the **service-session** keyword:

```
" tiered(1280000, 5120000)"
```

Related Documentation

- Service Session Profiles Overview on page 29
- Overview of Managing and Activating Service Sessions on page 11
- Overview of Managing Subscriber Service Sessions Using the CLI on page 13
- Activating Subscriber Sessions Using the CLI on page 51
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18
- Gracefully Deactivating Subscriber Service Sessions on page 54
- Forcing Immediate Deactivation of Subscriber Service Sessions on page 55

Understanding Service Manager RADIUS Attributes

For the RADIUS login method, the RADIUS VSAs for service activation, threshold configuration, statistics configuration, and interim accounting in Access-Accept messages at subscriber login are used by Service Manager to activate the appropriate service session. For the RADIUS CoA method, Service Manager uses the VSAs for service activation and deactivation, threshold configuration, statistics configuration, and interim accounting in CoA-Request messages to activate the service session. The accounting-related VSAs are included in RADIUS accounting messages.

Table 3 on page 15 lists the Service Manager-related attributes and indicates which are tagged VSAs. See "Using Tags with RADIUS Attributes" on page 17 for a discussion about using tagged VSAs to group attributes for a service.

Table 3: Service Manager RADIUS Attributes

Attribute Number	Attribute Name	RADIUS Message Type	VSA Description
[1]	User-Name (used with Virtual-Router, Juniper Networks VSA 26-1)	Access-Accept	Uniquely identifies the subscriber session
[8]	Framed-IP-Address (used with Virtual-Router, Juniper Networks VSA 26-1)	Access-Accept	Uniquely identifies the subscriber session
[26-65]	Activate-Service	Access-Accept and CoA-Request	Name of the service to be activated; includes parameter values; a tagged VSA
[26-66]	Deactivate-Service	Access-Accept and CoA-Request	Name of the service to be deactivated **Note:** This VSA is only used by CoA.
[26-67]	Service-Volume	Access-Accept and CoA-Request	Number of MB of traffic that the service can consume; the service is terminated when output byte count exceeds this value; a tagged VSA
[26-68]	Service-Timeout	Access-Accept and CoA-Request	Number of seconds that the service is to remain active; the service is terminated when the time expires; a tagged VSA
[26-69]	Service-Statistics	Access-Accept and CoA-Request	Statistics configuration; a tagged VSA: 0 = disable 1 = timestamp only 2 = timestamp and volume

Table 3: Service Manager RADIUS Attributes *(continued)*

Attribute Number	Attribute Name	RADIUS Message Type	VSA Description
[26-83]	Service-Session	For service sessions only: Acct-Start Acct-Stop Interim-Acct	Name of the service (including parameter values) with which the statistics are associated
[26-140]	Service-Interim-Acct-Interval	Access-Accept and CoA-Request	Number of seconds between accounting updates for a service; a tagged VSA
[31]	Calling-Station-ID	Access-Accept	Uniquely identifies the subscriber session
[44]	Acct-Session-ID	Acct-Start Acct-Stop Interim-Acct	Accounting identifier that makes it easy to match start and stop records in a log file; the format is extended to include a colon-separated value that uniquely identifies the subscriber session

NOTE: Service Manager statistics collection is a three-part procedure. You must configure statistics information in the service definition macro file, enable statistics collection in the RADIUS record, and also enable statistics collection for the policy referenced in the service macro using the **statistics enabled** keyword in the command used for policy attachment in the profile.

The Service-Volume and Service-Timeout VSAs rely on the values captured by the Service Manager statistics feature to determine when a threshold is exceeded. Therefore, you must configure and enable statistics collection to use these attributes. Service-Volume For detailed information about Service Manager statistics see "Configuring Service Manager Statistics" on page 71.

Table 4 on page 16 describes a partial RADIUS Access-Accept packet that activates a service session for subscriber client1@isp1.com. (The figure in "Creating Service Definitions" on page 41 shows the service definition macro file that creates the tiered service.) The session enables the subscriber to use the tiered service with an input bandwidth of 1280000 and output bandwidth of 5120000. The subscriber can use the service for 5 hours (18000 seconds), and Service Manager captures both timestamp and volume statistics during the session (service-statistics value of 2). Also, accounting for the service is updated every 600 seconds (10 minutes).

Table 4: Sample RADIUS Access-Accept Packet

RADIUS Attribute	Tag	Value
username	none	client1@isp1.com

Table 4: Sample RADIUS Access-Accept Packet *(continued)*

RADIUS Attribute	Tag	Value
class	none	(binary data)
service-activation	6	tiered(1280000, 5120000)
service-timeout	6	18000
service-statistics	6	2
service-interim-acct-interval	6	600

Using Tags with RADIUS Attributes

Service Manager uses tagged RADIUS VSAs to enable a single RADIUS record to activate multiple service sessions for a subscriber, with each session having unique attributes. A particular tag identifies a specific Activate-Service attribute and all other RADIUS attributes that are associated with that Activate-Service attribute.

You can specify a maximum of 8 tags (1–8), which enables you to activate up to eight unique service sessions for a subscriber in a single RADIUS record. The following are tagged VSAs—they must always have a tag in their RADIUS entry:

- Activate-Service
- Service-Statistics
- Service-Timeout
- Service-Volume
- Service-Interim-Acct-Interval

Table 5 on page 17 describes an Access-Accept packet that activates the two services, tiered and voice, for subscriber client1@isp1.com. Each service has its own unique tag, enabling you to assign attributes for one service, but not the other. For example, the two services have different timeout settings and different interim accounting intervals, and statistics are enabled only for the tiered service.

Table 5: Using Tags

RADIUS Attribute	Tag	Value
username	none	client1@isp1.com
class	none	(binary data)
service-activation	2	tiered(1280000, 5120000)
service-timeout	2	18000

Table 5: Using Tags *(continued)*

RADIUS Attribute	Tag	Value
service-statistics	2	1
service-interim-acct-interval	2	600
service-activation	6	voice(100000)
service-timeout	6	1440
service-interim-acct-interval	6	1200

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Overview of Managing and Activating Service Sessions on page 11
- Overview of Managing Subscriber Service Sessions Using RADIUS on page 12
- Understanding RADIUS Accounting for Service Manager on page 23
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48

Overview of Deactivating Subscriber Service Sessions Using the CLI

The CLI supports several methods that enable you to manually deactivate service sessions. You can:

- Gracefully terminate all services or a specific service for a particular subscriber
- Gracefully terminate all service or a specific service associated with a particular owner
- Force the immediate termination of all of a subscriber's sessions
- Use service session profiles to create time or volume thresholds for the service and deactivate the service when the threshold is reached. See "Service Session Profiles Overview" on page 29 and "Working with Service Session Profiles" on page 68.

NOTE: **You can use the CLI commands described in this topic to delete subscriber and service sessions that are created by either RADIUS or the CLI.**

The Service Manager CLI commands enable you to use variations of the **no service-management subscriber-session** command to terminate service sessions.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68

- Gracefully Deactivating Subscriber Service Sessions on page 54
- Forcing Immediate Deactivation of Subscriber Service Sessions on page 55
- Using Service Session Profiles to Deactivate Service Sessions on page 67

Overview of Activating and Deactivating Subscriber Services Using Mutex Groups

Service Manager supports two methods that use RADIUS CoA-Request messages to activate and deactivate subscriber services and that can also dynamically change a service that is currently provided to a subscriber.

In the first method, you use a CoA message with the Activate-Service VSA to activate the new service; you can optionally include the Deactivate-Service VSA to deactivate the subscriber's existing service. This method is described in "Activating Subscriber Service Sessions Using RADIUS" on page 47.

The second method uses mutual exclusion (mutex) groups to create mutex services. With this method, you group services together in a mutex group. When you use a CoA message to activate a service that is in a mutex group, Service Manager activates the new service and implicitly deactivates any existing service that it is a member of the same mutex group as the newly activated service. Service Manager does not deactivate an existing service that is a member of a different mutex group or is not a member of a mutex group.

Using mutex services results in an more reliable activation and deactivation process than the original CoA-Request method. With mutex services, Service Manager always activates the new service before deactivating the existing service. This ensures that the subscriber is never without an active service. In the original CoA-Request method, the order of activation and deactivation is random—in some cases the existing service might be deactivated before the new service is activated, or the new activation might fail. In these cases, the subscriber might be without an active service.

If statistics are enabled when you activate a mutex service, Service Manager sends a RADIUS Acct-Stop message for the deactivated service.

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48
- Configuring a Mutex Service on page 57
- Activating and Deactivating Multiple Services on page 57

CHAPTER 4

How Dual-Stack Subscriber Services Work

Combined and Independent IPv4 and IPv6 Services in a Dual Stack Overview

Internet Protocol version 6 (IPv6) is designed to enhance IP addressing and maintain other IPv4 functions that work well. Organizations worldwide are developing new applications to take advantage of the many feature enhancements within IPv6 to help bring back end-to-end controlled communications across a transparent network infrastructure. To ensure optimum performance, such applications implement a dual-stack architecture in which IPv4 and IPv6 protocols share a common transport and framing layer.

A dual-stack implementation supports both IPv4 and IPv6 hosts to help provide a smooth transition to all parts of a enterprise network. With this flexible method of implementation, providers can carry IPv6 traffic over their existing core networks and customers can roll out IPv6 to more sites.

The PPP link between the customer premises equipment (CPE) and the provider edge (PE) device or E Series router equipment might require both IPv4 and IPv6 protocols for transmission of data. Such networks require that PE devices run a dual stack of IPv4 and IPv6 services. In this release, the Service Manager application on the E Series router supports authentication, service selection, and service activation and deactivation to subscribers for both IPv4 and IPv6 protocols in a dual stack configuration.

You can configure services in a dual stack for IPv4 and IPv6 either independently or as a single entity. Service Manager only tracks JunosE objects that are passed back in the env.setResult method when a service definition is executed. In an IPv6 environment, you must modify the service definition macro file to include the objects that the Service Manager requires to categorize a service as IPv4, IPv6, or a combination of both IPv4 and IPv6.

You can use the **service-interface-type** object in the service definition macro file to specify whether a service must be defined for IPv4 or IPv6. Configuring the service-interface-type object is not mandatory if a service is required only for IPv4 or L2TP subscribers. However, you must specify the service-interface-type object when a service is required for IPv6 subscribers or IPv4 and IPv6 subscribers in a dual stack. After you create a new service definition file with the service-interface-type object and install it on the router, the Service Manager determines whether a service must be tagged as

IPv4, IPv6, or a combination of the two by parsing the objects passed using the macro environment command, **env.setResult**. The service-interface-type object can be configured with one of the following values:

- ipv4—Specifies that the service session profile must be applied to IPv4 interfaces only. This object is optional only when IPv4 or L2TP subscribers are in a network.
- l2tp—Specifies that the service session profile must be applied to L2TP interfaces. This object is optional only when IPv4 or L2TP subscribers are in a network.
- ipv4-ipv6—Specifies that the service session profile must be applied to both IPv4 and IPv6 interfaces in a dual stack. You must configure this object when IPv6 subscribers or IPv4/IPv6 subscribers in a dual stack are in a network.
- ipv6—Specifies that the service session profile must be applied to IPv6 interfaces only. You must configure this object when IPv6 subscribers or IPv4 and IPv6 subscribers in a dual stack are in a network.

When you create the service definition, include the following service attribute in the service definition if you want the service to be defined for IPv4 interfaces only. The profile identifier returned from the activate-profile object is applied to IPv4 interfaces.

```
<# env.setResult("service-interface-type", “ipv4” ) #>
```

To configure a service macro to be used for IPv6 interfaces only, specify the following object in the macro definition file. The profile identifier returned from the activate-profile object is applied to IPv6 interfaces.

```
<# env.setResult("service-interface-type", “ipv6” ) #>
```

To configure a service macro to be used for IPv4 and IPv6 interfaces in a dual stack, specify the following object in the macro definition file. The profile identifier returned from the activate-profile object is applied to both IPv4 and IPv6 interfaces.

```
<# env.setResult("service-interface-type", “ipv4-ipv6” ) #>
```

Related Documentation

- Service Definitions Overview on page 9
- Activation and Deactivation of IPv4 and IPv6 Services in a Dual Stack on page 61
- Service Interim Accounting for IPv4 and IPv6 Services in a Dual Stack Overview on page 27
- Example: Combined IPv4 and IPv6 Service in a Dual Stack Service Definition on page 95

CHAPTER 5

How Accounting with Service Manager Works

Understanding RADIUS Accounting for Service Manager

The Service Manager application supports RADIUS accounting and interim accounting for subscriber service sessions that are activated by the RADIUS login and RADIUS CoA methods. When RADIUS accounting is enabled, RADIUS generates:

- An Acct-Start message when a service session is activated
- An Acct-Stop message when a service session is deactivated
- Interim-Acct messages

RADIUS accounting messages always include Service Manager time statistics. You must enable Service Manager volume statistics for a service session.

When you terminate a subscriber session, Service Manager first sends RADIUS Acct-Stop messages for any active services associated with the subscriber session, and then sends the Acct-Stop message for the subscriber session.

NOTE: Service Manager statistics collection is a three-part procedure. You must configure statistics information in the service definition macro file, enable statistics collection by either RADIUS or the CLI, and also enable statistics collection for the policy referenced in the service macro using the **statistics enabled** keyword in the command for policy assignment to a profile at the time of attachment of the policy to an interface. For detailed information about Service Manager statistics, see "Configuring Service Manager Statistics" on page 71.

To support RADIUS accounting for Service Manager, the RADIUS Acct-Session-ID attribute [44] has been extended to include a colon-separated identifier, which uniquely identifies a service for a subscriber. For example:

```
erx FastEthernet 12/0:0001048580:002478
```

The Service-Session attribute (VSA 26-83) identifies the name of the service. This attribute is the value of the Activate-Service or Deactivate-Service attribute (including parameter values) that was used in the RADIUS Access-Accept message to activate or deactivate the service session. For example:

```
tiered(1280000, 5120000)
```

Table 6 on page 24 lists the RADIUS accounting attributes used by the Service Manager application.

Table 6: Service Manager RADIUS Accounting Attributes

Attribute Number	Attribute Name	RADIUS Message Type	VSA Description
[26-83]	Service-Session	For service sessions only: Acct-Start Acct-Stop Interim-Acct	Name of the service (including parameter values) with which the statistics are associated
[26-140]	Service-Interim-Acct-Interval	Access-Accept and CoA-Request	Number of seconds between accounting updates for a service; a tagged VSA
[44]	Acct-Session-ID	Acct-Start Acct-Stop Interim-Acct	Accounting identifier that makes it easy to match start and stop records in a log file; the format is extended to include a colon-separated value that uniquely identifies the subscriber session

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Understanding Service Manager RADIUS Attributes on page 15
- Service Interim Accounting Overview on page 24
- Configuring Service Interim Accounting on page 63
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48

Service Interim Accounting Overview

Interim accounting determines how often accounting information is updated and sent to an accounting server. In addition to the user-based interim accounting supported on

the router, Service Manager supports service-related interim accounting—you can configure an interim accounting interval for services that are created during a user RADIUS-based login and services that are activated by a CoA operation.

The service interim accounting interval is specified by the RADIUS Service-Interim-Acct-Interval attribute (VSA 26-140) that is included in the RADIUS Access-Accept message or CoA-Request message that activates a service session. Because the Service-Interim-Acct-Interval attribute is a tagged attribute, you can configure different interim accounting intervals for a particular user's various services.

You can use the **aaa service accounting interval** command to specify the default service interim accounting interval. Service Manager uses this interval value for service accounting when the Service-Interim-Acct-Interval attribute is not configured.

NOTE: You can also configure interim accounting for users. A user interim accounting interval is configured in the Acct-Interim-Interval RADIUS attribute (RADIUS attribute 85). You use the **aaa user accounting interval** command to specify the default user interim accounting interval, which is used when RADIUS attribute 85 is not configured. See the *Configuring Remote Access* chapter in this guide for information about configuring user interim accounting.

When the Service-Interim-Acct-Interval attribute is configured for a service, Service Manager uses the guidelines shown in Table 7 on page 25 to determine the correct interim accounting interval to use for the service.

Table 7: Determining the Service Interim Accounting Interval

Service-Interim-Acct-Interval Value	Service Manager Action
0	Disables interim accounting for the service
1–599	Uses 600
600–86400	Uses the specified value
86401 or greater	Uses 86400
The tag for the service-interim-acct-interval attribute does not match the tag for any service-activate attribute (VSA 26-65)	Discards the service-interim-acct-interval attribute

Table 8 on page 26 describes a sample Acct-Start message for a service session. In the table, the three fields used by Service Manager are shown in bold characters. An Acct-Start message for a subscriber session without any active services does not include the Service-Session attribute.

Table 8: Sample Acct-Start Message for a Service Session

RADIUS Attribute	Sample Value
acct-status-type	1
username	client1@isp1.com
event-timestamp	1112191723
acct-delay-time	0
nas-identifier	ERX-01-00-06
acct-session-id	**erx FastEthernet 12/0:0001048580:002478**
nas-ip-address	10.6.128.45
class	(binary data)
framed-protocol	0
framed-compression	0
framed-ip-address	100.20.0.1
framed-ip-netmask	0.0.0.0
ingress-policy-name (vsa)	forwardAll
egress-policy-name (vsa)	forwardAll
calling-station-id	#ERX-01-00-06#E12#0
acct-input-gigawords	0
acct-input-octets	4032
acct-output-gigawords	0
acct-output-octets	2163
acct-input-gigapackets (vsa)	0
acct-input-packets	7
acct-output-gigapackets (vsa)	0
acct-output-packets	7

Table 8: Sample Acct-Start Message for a Service Session *(continued)*

RADIUS Attribute	Sample Value
nas-port-type	15
nas-port	3221225472
nas-port-id	FastEthernet 12/0
acct-authentic	1
acct-session-time	0
acct-service-session	**tiered(1280000, 5120000)**
service-interim-acct-interval	**1200**

Related Documentation

- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- Service Interim Accounting for IPv4 and IPv6 Services in a Dual Stack Overview on page 27
- Configuring Service Interim Accounting on page 63

Service Interim Accounting for IPv4 and IPv6 Services in a Dual Stack Overview

You can query the external parent group statistics similar to the statistics retrieved for classifier lists. You must specify the correct external parent group name and its corresponding hierarchical policy parameter for each of the input, output, and secondary-input statistics. You can specify a list of external parent groups along with hierarchical policy parameter for which statistics must be collected and sent to Service Manager for display in the Acct-Stop and Interim-Acct messages. The statistics for packets arriving at an interface attached at the input stage and the statistics for packets arriving at an interface attached at the secondary input stage are added and displayed in the Input Bytes field of the **show service-management** command. The statistics for packets leaving an interface at which the hierarchical policy is defined are displayed in the Output Bytes field of the **show service-management** command. The external parent group statistics are not limited to combined IPv4 and IPv6 services in a dual stack. You can also obtain external parent group statistics for IPv4 and IPv6 services configured independently in a dual stack.

You can retrieve either external parent group statistics or classifier statistics from policy manager. However, you cannot retrieve both the statistics for a single service definition. When a combined service is configured, you cannot retrieve classifier list-based based statistics. In such a scenario, you can only retrieve external parent group-based statistics from policy manager.

Service interim accounting and accounting based on service deactivation are supported for IPv6 services. For the combined IPv4 and IPv6 service, the statistics are a sum of the values in the external parent group and hierarchical policy parameter pair lists (defined as input-stat-epg, secondary-input-stat-epg, and output-stat-epg in the service definition macro).

If an interface fails, service-related interim accounting does not calculate the packets that are transmitted through this failed interface. For statistics reporting, only those packets that exist for interfaces when the subscriber service session is deactivated are counted.

Related Documentation

- Understanding RADIUS Accounting for Service Manager on page 23
- Service Interim Accounting Overview on page 24
- Configuring Service Interim Accounting on page 63
- Combined and Independent IPv4 and IPv6 Services in a Dual Stack Overview on page 21
- Activation and Deactivation of IPv4 and IPv6 Services in a Dual Stack on page 61
- Example: Combined IPv4 and IPv6 Service in a Dual Stack Service Definition on page 95

CHAPTER 6

How Service Session Profiles Work

Service Session Profiles Overview

Service session profiles provide additional flexibility to the Service Manager application by enabling you to assign one or more supported attributes to a particular activation of a service.

For example, you might assign the same video service to two subscribers, but use different service session profiles to set different time limits for each subscriber's service. One subscriber uses the video service for 5 hours (18000 seconds) while the other subscriber's video service is for 10 hours (36000 seconds). Or, you might enable statistics on a subscriber's voice service and disable statistics on the same subscriber's video service.

You can create multiple service session profiles independent of the service activation process. Then, when you activate a service session, you specify the profile that you want to use with that particular service session—you can apply one profile to a service session.

You can configure the following attributes in service session profiles:

- **statistics**—Enables statistics and specifies the type of statistics you want to capture for the service. See "Configuring Service Manager Statistics" on page 71 for additional information about capturing Service Manager statistics. You can specify the following types of statistics:
  - **time**—The service's duration
  - **volume-time**—The service's duration and traffic volume
- **volume**—Specifies that the service is automatically deactivated when the indicated traffic volume is exceeded.
- **time**—Specifies that the service is automatically deactivated when the indicated time period is exceeded.

NOTE: The **volume** and **time** attributes use values captured by the Service Manager statistics feature to determine when the threshold is exceeded. Service Manager collects time statistics by default—you must configure and enable volume statistics collection. See "Configuring Service Manager Statistics" on page 71.

Related Documentation

- Working with Service Session Profiles on page 68
- Overview of Managing and Activating Service Sessions on page 11
- Overview of Managing Subscriber Service Sessions Using the CLI on page 13
- Overview of Activating Subscriber Service Sessions Using the CLI on page 14

CHAPTER 7

How HTTP Local Server for Guided Entrance Works

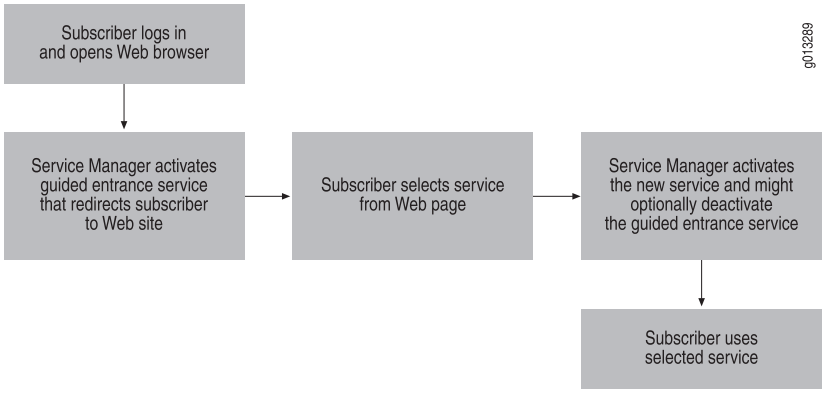
Guided Entrance Service Overview

The guided entrance service enables you to create a controlled Internet browsing environment. Guided entrance-based services, which are sometimes called *walled gardens* or *captive portals*, are becoming increasingly important offerings for service providers. When a subscriber logs in and opens a Web browser, the Service Manager guided entrance service transparently directs the subscriber to a specific Web site—at that Web site, the subscriber is presented with a selection of possible services to use. For example, a subscriber might be shown a Web site that offers services such as:

- Predefined services—A group of user-selectable services that meets a variety of needs of a single subscriber. The subscriber might select the high-priced highest access speed to perform critical financial transactions but select a lower speed (and lower cost) service for e-mail. For viewing a real-time sports event, the subscriber can select the video-on-demand service. The subscribers have control over the choice and cost of the services they need and use.
- Prepaid services—A group of specific services that have been prepaid by the subscriber. For example, a subscriber who has purchased the sports package service is presented with a Web page that lists the currently available sporting events. Or, a subscriber might prepay a VoIP service for a set amount of time.
- Controlled-service— An educational service that enables students at a school to access authorized research sites. Or, a limited service for young children that restricts access to safe, closely monitored, age-appropriate Web sites.

Figure 2 on page 32 shows the sequence of actions that take place during a guided entrance service.

Figure 2: Guided Entrance



Service Manager requires additional configuration considerations for the guided entrance service.

- The **<# redirectUrlName := "http://" $ serverIp $ ":" $ serverPort #>** command in the service definition—Specifies the HTTP local service to which the subscriber is redirected after login. See "Example: Guided Entrance Service Definition" on page 101 for a sample guided entrance service definition.

  NOTE: You must also configure a policy that redirects packets. See Creating an Exception Rule within a Policy Classifier Group in *JunosE Policy Management Configuration Guide* for information on creating redirect policies.

- HTTP local server application—Used by the policy in the activated service to direct a subscriber to a specific Web site when the subscriber logs in. See "Configuring the HTTP Local Server to Support Guided Entrance" on page 87 for information about the HTTP local server.
- RADIUS Dynamic Request Server and CoA messages—Enables RADIUS to dynamically activate the new service that the subscriber selects at the Web site. Can also optionally deactivate the original guided entrance service session that is used when the subscriber logs in. See the *Configuring RADIUS Dynamic-Request Server* chapter in this guide.

Related Documentation

- Using CoA Messages with Guided Entrance Services on page 91
- Example: Guided Entrance Service Definition on page 101

Redirection of Subscriber Sessions When HTTP Local Server is Disabled or Not Configured

The HTTP local server on the router must always be enabled before the subscriber logs in for the redirect URL to be returned. If the HTTP local server is activated on the router after the subscribers have logged in, the URL to which the subscriber's Web browser session needs to be redirected is not returned to the users. Instead, the redirect engine

opens a TCP port (8800 by default) and sends an HTTP 302 Found response to the subscriber's browser in response to the request. The subscriber must log out and log in again for the redirection URL to be returned to the subscriber in response to the initial request.

The HTTP redirect URL functionality works correctly only if the HTTP local server is running on the system before subscribers log in. Also, if the HTTP local server is disabled and reenabled, previously logged-in subscribers must log out and reestablish their sessions for the redirect URL to be returned. After you disable and reenable the HTTP local server on the router, the interface configuration details for previously logged-in subscribers are not retained.

Consider a scenario in which two subscribers, subscriber A and subscriber B, are logged in, the HTTP local server for both IP and IPv6 traffic is enabled on the router, and URL redirection functionality is configured. In such a topology, when subscriber A sends an HTTP GET request to the HTTP local server on the router, the subscriber's HTTP session is redirected to the configured URL. If you disable the HTTP local server for IP traffic by using the **no ip http server** command and reenable the HTTP local server by using the **ip http server** command, when subscriber B sends an HTTP GET request to the router, the session is not redirected to the configured URL. The user session is redirected to the correct configured site only when subscriber B logs out and logs back in again.

Related Documentation

- Guided Entrance Service Overview on page 31
- Configuring the HTTP Local Server to Support Guided Entrance on page 87
- Example: Guided Entrance Service Definition on page 101

Preservation of the Original URL During Redirection of Subscriber Sessions

When guided entrance service is used and a digital subscriber line (DSL) user logs in for the first time and opens a Web browser, the subscriber is directed to a specific URL for user provisioning. Provisioning involves application of a service definition which enables all HTTP traffic to be handled temporarily by the HTTP local server. After the provisioning process, the service definition is removed and traffic no longer flows to the HTTP local server. At this point, the user is redirected to the original requested URL. The HTTP local server redirect feature supports the preservation of the original URL as a variable in the redirect URL. If preservation of the original URL feature is enabled, then the user's HTTP session is directed back to the URL which was requested before the redirection.

Related Documentation

- Configuring the Preservation of the Original URL During Redirection of Subscriber Sessions on page 92

CHAPTER 8

Service Manager Performance Considerations

Service Manager Performance Considerations

Like any application, Service Manager requires a certain amount of system resources. Consider the following guidelines to maximize the performance of Service Manager when delivering subscriber services:

- Minimize service definitions—Use the minimum number of JunosE commands in a service definition to specify a service.
- Reference objects in service definitions—Referencing commonly used objects is more resource-efficient than using unique objects for each subscriber (for example, using a subscriber's IP address as a match criteria in a classifier list).
- Preprovision frequently used services— Preprovisioning saves resources by requiring Service Manager to build a popular service only once. You then reuse the original service when you activate future subscriber service sessions. See "Preprovisioning Service Sessions" on page 53 for details.
- Capture volume statistics when needed—Repeatedly capturing volume statistics can waste resources.

Related Documentation

- Service Definitions Overview on page 9
- Overview of Referencing Policies in Service Definitions on page 8
- Creating Service Definitions on page 41
- Service Session Profiles Overview on page 29
- Preprovisioning Service Sessions on page 53

PART 2

Configuration

CHAPTER 9

Configuration Tasks for Service Manager

Configuring the Service Manager License

Use the Service Manager license to enable full Service Manager application support. You can create a maximum of 10 subscriber sessions when the Service Manager license is not enabled. If you disable the Service Manager license and more than 10 subscriber sessions exist, you cannot enable any new sessions—however, all existing active subscriber sessions continue to function.

For information about the maximum number of subscriber sessions supported, see *JunosE Release Notes, Appendix A, System Maximums*.

To specify the Service Manager license and enable full Service Manager application support—if the license is not enabled, you are limited to 10 subscriber sessions:

NOTE: **Obtain the license from Juniper Networks Customer Service or your Juniper Networks sales representative.**

- Issue the **license service-management** command in Global Configuration mode.

  host1(config)#license service-management 123456789

  The license is a unique string of up to 15 alphanumeric characters.

  Use the **no** version to disable the license.

Related Documentation

- Configuring Service Manager
- Managing Your Service Definitions on page 44
- license service-management

CHAPTER 10

Configuration Tasks for Service Definitions

Creating Service Definitions

To create a service definition, you use the JunosE Software's macro language to specify the parameters that define the desired service. A macro file can define only one service—however, the file can have multiple templates to define characteristics of the desired service. You create service definitions independent of the Service Manager commands and operations, which are performed on the E Series router.

For detailed information about the JunosE Software's macro language, see the *Command Line Interface* chapter in *JunosE System Basics Configuration Guide*.

Figure 3 on page 43 is an example of a service definition macro file that creates a tiered service. A tiered service typically provides set bandwidths for both inbound and outbound traffic for a subscriber. In this example, the input (inputBW) and output (outputBW) bandwidth values are parameterized. This example assumes that QoS profile triplePlayIP and QoS parameter maxSubscBW are configured. See "Example: Video-on-Demand Service Definition" on page 106, "Example: Voice-over-IP Service Definition" on page 108, and "Example: Guided Entrance Service Definition" on page 101 for additional service definition examples.

Service Manager only tracks JunosE objects that are passed back in the env.setResult method when a service definition is executed. Table 9 on page 41 describes the supported objects:

Table 9: JunosE Objects Tracked by Service Manager

Name	Requirement	Description
input-stat-clacl	Optional	• Collects input statistics from policy manager • Can be a list of clacls
secondary-input-stat-clacl	Optional	• Collects input statistics from policy manager • Can be a list of clacls

Table 9: JunosE Objects Tracked by Service Manager *(continued)*

Name	Requirement	Description
output-stat-clacl	Optional	• Collects output statistics from policy manager • Can be a list of clacls
activate-profile	Required	• Specifies the interface profile used on activation of the service • Deletion of the profile is Service Manager's responsibility
deactivate-profile	Optional	• Specifies the interface profile used on deactivation of the service • If not specified, is the same as the activation-profile • Deletion of the profile is Service Manager's responsibility
command-in-error	Optional	• Passes the value env.getErrorCommand • Service Manager displays the line in the service definition that has the error
command-error-status	Optional	• Passes the value env.getErrorStatus • Service Manager displays the error status for the error
service-interface-type	• Optional for IPv4 or L2TP services • Mandatory for independent IPv6 services or combined IPv4 and IPv6 services in a dual stack	• Specifies the type of interface, IPv4, IPv6, combination of IPv4 and IPv6, or L2TP, to which the service session profile must be applied
input-stat-epg	Optional	• Collects input statistics associated with the external group from policy manager • Both the external parent group and the corresponding hierarchical policy parameter must be specified • Can be multiple pairs of external parent groups and hierarchical policy parameters

Table 9: JunosE Objects Tracked by Service Manager *(continued)*

Name	Requirement	Description
output-stat-epg	Optional	• Collects output statistics associated with the external group from policy manager • Both the external parent group and the corresponding hierarchical policy parameter must be specified • Can be multiple pairs of external parent groups and hierarchical policy parameters
secondary-input-stat-epg	Optional	• Collects input statistics associated with the external group that is attached at the secondary input stage from policy manager • Both the external parent group and the corresponding hierarchical policy parameter must be specified • Can be multiple pairs of external parent groups and hierarchical policy parameters

Figure 3: Sample Service Definition Macro File

```
!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>


classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
    committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
    classifier-group matchAll precedence 10000
        rate-limit-profile <# name; '\n' #>
        traffic-class best-effort

policy-list <# oname; '\n' #>
    classifier-group matchAll precedence 10000
        traffic-class best-effort

profile <# name; '\n' #>
    ip policy secondary-input <# name #> statistics enabled merge
    ip policy output <# oname #> statistics enabled merge
    qos-profile triplePlayIP
    qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clacl", "matchAll") #>
<# env.setResult("output-stat-clacl", "matchAll") #>

<# endtmpl #>
```

Related Documentation

- Service Definitions Overview on page 9

Managing Your Service Definitions

After you have created the macro file for your service definition, you can perform the following operations with the service definition macro file:

NOTE: All new service sessions will be activated using the new service definition. Any existing service sessions that were activated using the original service definition continue to use the original definition until you deactivate the service session.

Copying a Service Definition Macro File

You must copy the service definition from the local computer that you used to create the macro file to the router's NVS card.

To copy a service definition macro file from your computer to the router's NVS:

- Issue the **copy** command in Privileged Exec mode. You must specify the directory containing the macro file you want to copy and the name you want to use for the file in NVS.

  host1#copy boston:/serviceDefs/triplePlay/tiered.mac tiered.mac

  There is no **no** version.

Installing a Service Definition File

You must install the service definition before you can use it to create a service session. During installation, Service Manager precompiles the definition and extracts and extracts the definition file's timestamp. Precompiling the service definition improves Service Manager performance. The timestamp enables the Service Manager application to track any modifications you might make while the definition is being used.

To install a service definition file:

- Issue the **service-management install** command in Global Configuration mode.

  host1(config)#service-management install tiered.mac

You must include the .mac extension while you use the **service-management install** command to install a service definition. After you install the service definition, you can use the definition to create service sessions for subscribers.

Use the **no** version of this command to remove a previously configured service definition.

Uninstalling a Service Definition File

You can uninstall a service definition file, for example, if you no longer want to use that definition. When you uninstall a service definition file, any existing service sessions that were activated using the original service definition continue to use the original definition until you deactivate the service session.

To uninstall a service definition file:

- Issue the **no service-management install** command in Global Configuration mode.

```
host1(config)#no service-management install tiered.mac
```

Updating an Existing Service Definition File

You can update an existing service definition file at any time. To update a service definition file:

To update an existing service definition, you make changes to the original macro file on your computer, copy the updated file to NVS, and install the updated file. All subsequent service sessions use the new service definition file. However, currently active service sessions continue to use the original definition file until the sessions are deactivated, then reactivated.

1. Use your text editor on your computer to make changes to the original service definition file.
2. Copy the updated service definition file back to your router's NVS—this overwrites the original file on the router.

```
! update the original macro file on the remote system


! copy the updated macro file to the router
host1#copy boston:/serviceDefs/triplePlay/tiered.mac tiered.mac
```

3. Enter the Global Configuration mode and Install the new service definition file.

```
host1#configure terminal
! install the updated service definition on the router
host1(config)#service-management install tiered.mac
```

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Referencing QoS Configurations in Service Definitions on page 77
- Specifying QoS Profiles in Service Definitions on page 78
- Example: Tiered Service Definition on page 104

- Example: Voice-over-IP Service Definition on page 108
- Example: Video-on-Demand Service Definition on page 106
- Example: Guided Entrance Service Definition on page 101
- **copy on page 114**
- **service-management install on page 129**

CHAPTER 11

Configuration Tasks for Service Sessions Using RADIUS

Activating Subscriber Service Sessions Using RADIUS

To use RADIUS to activate subscriber service sessions, you create a RADIUS record that includes the Activate-Service VSA. For the RADIUS login method, this RADIUS record is used by the Access-Accept message to start Service Manager and activate the service when the subscriber logs in.

For the RADIUS CoA method, the service provider uses a CoA-Request message to activate and deactivate the service for the subscriber who is already logged in.

To configure a service session that will be activated by RADIUS:

1. Create the RADIUS record for the subscriber and service:
   - For RADIUS login—Create the RADIUS record for the subscriber and include the Activate-Service VSA in the record. Specify values for the parameters defined in the service template name of the definition macro file.
   - For RADIUS CoA—Format the CoA message to create the RADIUS record for the subscriber. Include the Activate-Service VSA in the record. Optionally, include the Deactivate-Service VSA if the subscriber has an active service session that you want to deactivate. Specify values for the parameters defined in the service template name of the definition macro file.

NOTE: You specify the parameter values in the order in which the parameters appear in the template name of the service definition file. For example, in the tiered service that is defined in the sample service definition macro file in "Creating Service Definitions" on page 41, the template name is:

```
<# tiered(inputBW, outputBW) #>
```

For the RADIUS Activate-Service VSA, you specify values for the input and output bandwidth:

```
tiered(1280000, 5120000)
```

2. Specify optional VSAs for the service session as needed:
   - Service-Volume
   - Service-Timeout
   - Service-Statistics

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Deactivating Service Sessions Using RADIUS on page 48
- Overview of Activating and Deactivating Subscriber Services Using Mutex Groups on page 19
- Activating and Deactivating Multiple Services on page 57

Deactivating Service Sessions Using RADIUS

You can deactivate a service session by using a CoA-Request message or when a subscriber logs out of a RADIUS-activated service session. If the subscriber logs off the router, Service Manager deactivates that subscriber session and all associated service sessions.

RADIUS also supports attributes that you can use to manage deactivation of service sessions. You can deactivate service sessions with the following set of tasks:

- Setting Time or Volume Thresholds for a Service on page 48
- Using the Deactivate-Service Attribute on page 49

Setting Time or Volume Thresholds for a Service

You can set a threshold for the session by including one or both of the following attributes in the RADIUS record:

NOTE: The Service-Timeout and Service-Volume attributes use values captured by the Service Manager statistics feature to determine when a threshold is exceeded. Therefore, you must configure and enable statistics collection to use these attributes. See "Configuring Service Manager Statistics" on page 71.

- Service-Timeout—The number of seconds that the service session is active. You can specify a number in the range 0–16777215. Values greater than 16777215 are recycled, starting from the initial value of 0. For example, if you specify the value for Service-Timeout VSA as 16777218, this value is equivalent to 2 for this VSA. A value of 0 indicates that the session never times out. A particular Service-Timeout VSA can be used by a maximum of 2000 services.

  The service-timeout threshold accuracy is within 30 seconds of the specified value.

- Service-Volume—The total number of MB of traffic that can use the service session. You can specify a number in the range 0–16777215 MB. Values greater than 16777215 are recycled, starting from the initial value of 0. A value of 0 indicates that there is no limit to the amount of traffic for the session. For example, if you specify the value for Service-Timeout and Service-Volume VSAs as 16777216 and 16777217, these values are equivalent to 0 and 1 respectively for these VSAs. A particular Service-Volume VSA can be used by a maximum of 1000 services.

  NOTE: Service Manager terminates a session when the *output* byte count exceeds the configured service-volume threshold. The output byte count is captured by the **output-stat-clacl** string in the classifier list variable that you configure to collect statistics. See "Configuring Service Manager Statistics" on page 71.

  The service-volume threshold accuracy is based on a 10-second period. Service Manager does not immediately deactivate a service session when the output byte count reaches the service-volume threshold. Instead, Service Manager checks the volume in 10-second intervals and deactivates a service session at the end of the 10-second period in which the output byte count reaches the volume threshold. For example, if a threshold is reached 4seconds into the 10-second interval, the session continues for the remaining 6 seconds in the measuring period and is then terminated. Therefore, the total volume equals the threshold plus the volume during the additional 6 seconds.

When the output byte count reaches the threshold, RADIUS deactivates the service session. You must use tags to associate threshold attributes with the Activate-Service attribute for the service session.

Using the Deactivate-Service Attribute

You can also include the Deactivate-Service attribute in the subscriber's RADIUS record. The format for this attribute is the same as the format of the Activate-Service attribute—the name of the service, including parameters. The Deactivate-Service attribute

is used by RADIUS CoA messages, such as in a guided entrance service. See "Example: Guided Entrance Service Definition" on page 101 for more information.

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Overview of Activating and Deactivating Subscriber Services Using Mutex Groups on page 19
- Activating and Deactivating Multiple Services on page 57

CHAPTER 12

Configuration Tasks for Service Sessions Using CLI

Activating Subscriber Sessions Using the CLI

You can use the CLI to activate a service session based on subscriber information or owner information. You can activate a service session by performing one of the following tasks:

Activating a Service for an Existing Subscriber

You can use the **service-management owner-session** command to activate a service for an existing subscriber by identifying the owner used to create the subscriber session and specifying the service session to use. The subscriber session must exist before you use this command.

You can use this command in Privileged Exec mode to create a dynamic subscriber session—dynamic sessions are deleted after a router reboot. You can use this command in Global Configuration mode to create persistent subscriber sessions that are retained across reboots.

You can specify the name of the owner (the method originally used to create the subscriber session), and the ID generated by the of the owner. For example, if RADIUS was used to create the subscriber session, the owner name is AAA and the owner ID is the Acct-Session-ID generated by RADIUS when the subscriber session was created.

You can activate one subscriber session for a subscriber—and multiple service sessions for a particular subscriber session. If you create a second subscriber session for the same subscriber, only the newest subscriber session, with its services, is used.

You can include the optional **service-session-profile** keyword to assign a profile to the service session. The service session profile includes additional attributes, such as the type of statistics to be captured for the service session.

- To activate a service session for an existing subscriber:

  ```
  host1(config)#service-management owner-session aaa 573498 service-session
    "video(4500000, 192.168.10.3)"
  ```

- To activate multiple service sessions for an existing subscriber:

  ```
  host1(config)#service-management owner-session aaa 573498 service-session
    "video(4500000, 192.168.10.3)"
  host1(config)#service-management owner-session aaa 573498 service-session
    "tiered(1000000, 2000000)"
  host1(config)#service-management owner-session aaa 573498 service-session
    "voice(1000000, 10.10.10.1)"
  ```

- To include a service session profile when you activate a subscriber's service session:

  ```
  host1(config)#service-management owner-session aaa 426777 service-session
    "video(4500000, 192.168.10.3)" service-session-profile vodISP1
  ```

Use the **no** version to deactivate service sessions based on owner information. See "Overview of Deactivating Subscriber Service Sessions Using the CLI" on page 18 for more information about deactivating subscriber service sessions.

Creating and Activating a Service for a Subscriber

You can use the **service-management subscriber-session service-session** command to activate a service for a subscriber by creating a subscriber session and a service session.

NOTE: Always activate at least one service session for a subscriber session. The ability to create a subscriber session without a service session (by omitting the **service-session** keyword) is not currently supported.

You can use this command in Privileged Exec mode to create a dynamic subscriber session—dynamic sessions are deleted after a router reboot. You can use this command in Global Configuration mode to create persistent subscriber sessions that are retained across reboots.

You can create one subscriber session for a subscriber—and multiple service sessions for a particular subscriber session. If you create a second subscriber session for the same subscriber, only the newest subscriber session, with its services, is used.

You can include the optional **service-session-profile** keyword to assign a profile to the service session. The service session profile includes additional attributes, such as the type of statistics to be captured for the service session.

- To activate a subscriber session with a single service session:

  ```
  host1(config)#service-management subscriber-session client1@isp1.com  interface
    atm 4/0.1 service-session "video(4500000, 192.168.10.3)"
  ```

- To activate a single subscriber session with multiple service sessions:

```
host1(config)#service-management subscriber-session client1@isp1.com interface
  atm 4/0.1 service-session “video(4500000, 192.168.10.3)”
host1(config)#service-management subscriber-session client1@isp1.com interface
  atm 4/0.1 service-session “tiered(1000000, 2000000)”
host1(config)#service-management subscriber-session client1@isp1.com interface
  atm 4/0.1 service-session “voice(1000000, 10.10.10.1)”
```

- To include a service session profile when you activate a subscriber’s service session:

```
host1(config)#service-management subscriber-session client1@isp1.com interface
  atm 4/0.1 service-session “video(4500000, 192.168.10.3)” service-session-profile
  vodISP1
```

- Use the **no** version to deactivate service sessions. See “Overview of Deactivating Subscriber Service Sessions Using the CLI” on page 18 for more information about deactivating subscriber service sessions.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Overview of Managing Subscriber Service Sessions Using the CLI on page 13
- Overview of Activating Subscriber Service Sessions Using the CLI on page 14
- Preprovisioning Service Sessions on page 53
- **service-management subscriber-session service-session on page 132**

Preprovisioning Service Sessions

Preprovisioning service sessions is a technique you can use to improve Service Manager’s performance. Typically, when you use a service definition to activate a subscriber’s service session, Service Manager uses resources to build that service. However, if you later use the same service definition to activate a service session for a second subscriber, Service Manager does not have to rebuild the service—it bases the new service on the service that it built for the first service session. After you deactivate the first session, Service Manager must build a new service for any subsequent subscribers.

Preprovisioning entails activating a service for a dummy user on the null interface. You can then use the preprovisioned service session to activate service sessions for actual subscribers. This technique improves performance because you only require Service Manager to build the service one time, then reuse the original service when you activate future subscriber service sessions.

To preprovision a service you use a command similar to the following example:

```
host1(config)#service-management subscriber-session dummy interface null
  service-session “tiered(1000000, 2000000)”
```

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Activating Subscriber Sessions Using the CLI on page 51

Gracefully Deactivating Subscriber Service Sessions

You can deactivate a specific service for a subscriber, or you can delete a subscriber session, which deactivates all of the subscriber's service sessions. We recommend you use this command to deactivate subscriber service sessions.

You can gracefully deactivate subscriber service sessions using one of the following tasks:

Gracefully Deactivating Service Sessions Based on Owner Details

You can use the **no service-management owner-session** command to gracefully deactivate service sessions for a subscriber based on owner information.

To gracefully deactivate service sessions for a subscriber based on owner information:

- Issue the **no service-management owner-session** command in Global Configuration mode by specifying the owner name and owner ID of the service session you want to deactivate.

  host1(config)#no service-management owner-session aaa 426777 service-session "video(4500000, 192.168.10.3)"

  You can use the **no** version with the **service-session** keyword to deactivate the specified service session. You can use the **no** version *without* the **service-session** keyword to delete the subscriber's session and deactivate all of the subscriber's service sessions.

Gracefully Deactivating Service Sessions Based on Subscriber Details

You can use the **no service-management subscriber-session** command to gracefully deactivate service sessions for a subscriber based on the subscriber credentials.

To gracefully deactivate service sessions for a subscriber based on the subscriber's username and interface, and not the subscriber session ID:

- Issue the **no service-management subscriber-session** command in Global Configuration mode by specifying the owner name and owner ID of the service session you want to deactivate.

  host1(config)#no service-management subscriber-session client1@isp1.com interface atm 4/0.1 service-session "tiered(1000000, 2000000)"

  You can use the **no** version without the **service-session** keyword to delete the subscriber's session and deactivate all of the subscriber's service sessions. You can

use the **no** version with the **service-session** keyword to deactivate the specified service session.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Activating Subscriber Sessions Using the CLI on page 51
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18
- Forcing Immediate Deactivation of Subscriber Service Sessions on page 55
- Using Service Session Profiles to Deactivate Service Sessions on page 67

Forcing Immediate Deactivation of Subscriber Service Sessions

You can force the immediate deactivation of the specified subscriber session. Such an action deletes all active service sessions for the subscriber. We recommend this method if you encounter difficulty when you used the graceful deactivation method. Always use the graceful method first.

To force the immediate termination of a subscriber session and to deactivate all services for the specified subscriber session:

- Issue the **no service-management subscriber-session** command in Global Configuration mode by specifying the subscriber session ID with the **force** keyword.

```
host1(config)#no service-management subscriber-session 8 force
```

NOTE: To determine the subscriber session ID of a session you want to deactivate, use the **show service-management subscriber-session brief** command. The display lists the IDs of all active subscriber sessions and the owner that created the session, such as AAA (RADIUS) or CLI.

There is no affirmative version of this command; there is only a **no** version.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Activating Subscriber Sessions Using the CLI on page 51
- Preprovisioning Service Sessions on page 53
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18
- Gracefully Deactivating Subscriber Service Sessions on page 54
- Using Service Session Profiles to Deactivate Service Sessions on page 67
- **service-management owner-session on page 131**
- **service-management subscriber-session service-session on page 132**

CHAPTER 13

Configuration Tasks for Mutex Services

Activating and Deactivating Multiple Services

The Service Manager mutex service feature enables you to activate and deactivate multiple services with a single CoA-Request message. A CoA-Request message can have more than one service activation request—the multiple service requests might be from the same mutex group or from different groups. The following examples describe how you might use mutex groups to activate and deactivate multiple services.

- Case 1—Multiple mutex services of the same mutex group

  Service Manager activates the multiple mutex services, which are in the same group, then deactivates all previously existing services that are also members of that mutex group. Active services that are members of different mutex groups are unaffected.

- Case 2—Multiple mutex services of different mutex groups

  Service Manager activates the mutex services, which are members of different mutex groups. Service Manager then deactivates all previously existing services that are members of the same mutex groups as any of the newly activated services. Active services that are members of different mutex groups are unaffected.

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48
- Overview of Activating and Deactivating Subscriber Services Using Mutex Groups on page 19
- Configuring a Mutex Service on page 57

Configuring a Mutex Service

To configure and enable a mutex service, you complete the following steps:

1. Create the new service definition and configure the service as a member of a mutex group.

   When you create the service definition, include the following service attribute in the service definition, where groupIndex identifies the mutex group for this service. The groupIndex can be a number in the range -1 to - 2147483647 or 1 to 2147483646. If the groupIndex is outside of the acceptable ranges, or if you do not include the mutex-group statement, the service is not included in a mutex group.

   <# env.setResult("mutex-group", "*groupIndex*") #>

   For example (the mutex group attribute is highlighted in bold text):

```
!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>

classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
classifier-group matchAll precedence 10000
rate-limit-profile <# name; '\n' #>
traffic-class best-effort

policy-list <# oname; '\n' #>
classifier-group matchAll precedence 10000
traffic-class best-effort

profile <# name; '\n' #>
ip policy secondary-input <# name #> statistics enabled merge
ip policy output <# oname #> statistics enabled merge
qos-profile triplePlayIP
qos-parameter maxSubscBW <# outputBW; '\n' #>


<# env.setResult("mutex-group", "12" ) #>
<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clacl", "matchAll") #>
<# env.setResult("output-stat-clacl", "matchAll") #>

<# endtmpl #>
```

2. Activate the mutex service

   Use a RADIUS CoA-Request message and the new service definition to create the mutex service. The new service is considered a mutex service because it belongs to a mutex group.

   Service Manager activates the new service and deactivates any existing active service that is a member of the same mutex group as the new service.

3. (Optional) Verify the status of the new service.

```
host1# show service-management subscriber-session client1@isp.com interface ip 192.168.0.1
User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1
 Id: 1
 Owner: AAA 4194326
 Non-volatile: False
 State: Active
```



```
 ServiceSessions:
       Name             mutex  Owner/Id     State              Operation
----------------------- -----  ----------- ------------------  ---------
tiered(2000000,3000000)  12   AAA 4194326  ConfigApplySuccess  Activate
       Name             Non-volatile
----------------------- ------------
tiered(2000000,3000000)   False
```

Related Documentation

- Service Session Profiles Overview on page 29
- Understanding Service Manager RADIUS Attributes on page 15
- Activating Subscriber Service Sessions Using RADIUS on page 47
- Deactivating Service Sessions Using RADIUS on page 48
- Overview of Activating and Deactivating Subscriber Services Using Mutex Groups on page 19
- Activating and Deactivating Multiple Services on page 57

CHAPTER 14

Configuration Task for Dual-Stack Subscriber Services

Activation and Deactivation of IPv4 and IPv6 Services in a Dual Stack

You can configure IPv4 and IPv6 services in a dual stack either as independent services or as a combined service. The following sections describe the two types of configurations and their behavior when they are activated and deactivated.

Independent IPv4 and IPv6 Services in a Dual Stack

To configure separate services for IPv4 and IPv6 interfaces you must create and install separate service definitions on the router. For example, you can create a service definition called iponeV4 to be used for IPv4 traffic and service definition called iponeV6 to be used for IPv6 traffic. Both the services defined for IPv4 and IPv6 must be configured for the subscriber on the RADIUS server. When the subscriber is authenticated using RADIUS authentication, two services, one each for IPv4 and IPv6, are created. The subscriber service sessions are created and activated when the subscriber logs in using the RADIUS Access-Accept messages, Change-of-Authorization-Request (CoA-Request) messages, or CLI commands. After the subscriber service session is activated, the policies defined in the interface profile specified by the activate-profile object in the service macro file are applied to the IPv4 and IPv6 interfaces. Service session profiles provide additional flexibility to the Service Manager application by enabling you to assign one or more supported attributes to a particular activation of a service.

Deactivation of service sessions is also performed for each individual service. If an interface is deleted, all the services associated with that interface are also deleted. For example, if you delete an IPv6 interface, all the services associated with IPv6 are deleted. However, IPv4 subscriber service sessions are not disrupted. When a user logs out of a session, all services associated with the subscriber session are also removed along with the subscriber session. If the subscriber has two services and one of them was not successfully applied to an interface, then that service is removed. For example, if a subscriber has two services, iponev4 and iponev6, configured on the RADIUS server and only one service was successfully configured on an interface, then the failed service is deleted when the service is deactivated.

Combined IPv4 and IPv6 Service in a Dual Stack

To configure a single service for IPv4 and IPv6 interfaces, you can create and install one service definition on the router that handles the traffic for both these protocols. For example, you can create a service definition called iponeV4V6 to be used for both IPv4 and IPv6 traffic. This service must be configured for the subscriber on the RADIUS server. When the subscriber is authenticated using RADIUS authentication, a single service is created and activated using the RADIUS or CLI client type that Service Manager supports. After the subscriber service session is activated, the policies defined in the interface profile specified by the activate-profile object in the service macro file are applied to both IPv4 and IPv6 interfaces. The elements in the profile to be attached to the interfaces are determined by the type of the interface. The combined service session is active if either of the two conditions is satisfied:

- Both the IPv4 and IPv6 interfaces are up
- Either the IPv4 or IPv6 interface is up

Deactivation of service sessions results in disconnection of services for both IPv4 and IPv6 subscribers.

Performance Impact on the Router and Compatibility with Previous Releases for an IPv4 and IPv6 Dual Stack

In an environment where only IPv4 subscribers exist, the memory usage on the E Series router is the same as the usage in previous releases. If IPv4 and IPv6 are configured as independent services, memory usage increases because each IPv6 service is counted as a separate service and uses all the system resources than an IPv4 service requires. Memory impact in such a case is proportional to the total number of services configured. You can view the number of service sessions currently active for a subscriber by viewing the Service Sessions field from the output of the **show service-management** command.

If you configured a combined IP4 and IPv6 service, the memory usage is the same as that required for one subscriber service session. The number of subscribers that are supported by the line modules depends on the number of available resources, such as external parent groups. If you configure services that are to be used in an IPv4 or L2TP network, you need not change the previously defined service macros. However, if a subscriber requires the service macro applied to IPv6 interfaces or wants to apply a combined policy for both IPv4 and IPv6 interfaces, you must modify the macro file for the appropriate service interface type.

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Combined and Independent IPv4 and IPv6 Services in a Dual Stack Overview on page 21
- Example: Combined IPv4 and IPv6 Service in a Dual Stack Service Definition on page 95

CHAPTER 15

Configuring Accounting for Service Manager

Configuring Service Interim Accounting

You can configure user-based interim accounting on the router. In addition, you can configure service-related interim accounting for services that are created during a user RADIUS-based login and services that are activated by a CoA operation.

Configuring service interim accounting comprises the following sets of tasks:

Specifying the Service Accounting Interval

You can specify the default interval between service accounting updates by using the **aaa service accounting interval** command. Service manager uses the default interval when no value is specified in the Service-Interim-Acct-Interval attribute (Juniper VSA 26-140).

To specify the default interval between service accounting updates:

- Issue the **aaa service accounting interval** command in Global Configuration mode.

  host1(config)#aaa service accounting interval 60

  You can specify the service accounting interval in the range of 10–1440 minutes. The default setting is 0, which disables the feature.

NOTE: To enable interim service accounting, the service accounting interval must be set to a non-zero value and the service statistics type must *not* be set to *none*.

This command and the **aaa user accounting interval** command replace the **aaa accounting interval** command, which is deprecated and might be removed in a future release. The default interval is applied on a virtual router basis—this setting is used for services associated with all users who attach to the corresponding virtual router.

Use the **no** version to reset the accounting interval to 0, which turns off interim service accounting when no value is specified in the Service-Interim-Acct-Interval attribute (Juniper VSA 26-140).

Specifying the User Accounting Interval

You can specify the default interval between user accounting updates by using the **aaa user accounting interval** command. The router uses the default interval when no value is specified in the RADIUS Acct-Interim-Interval attribute (RADIUS attribute 85).

To specify the default interval between user accounting updates:

- Issue the **aaa user accounting interval** command in Global Configuration mode.

  host1(config)#aaa user accounting interval 20

  The default interval is applied on a virtual router basis—this setting is used for all users who attach to the corresponding virtual router. You can specify the user accounting interval, in the range 10–1440 minutes. The default setting is 0, which disables the feature.

  This command and the **aaa service accounting interval** command replace the **aaa accounting interval** command, which is deprecated and might be removed in a future release.

  Use the **no** version to reset the accounting interval to 0, which turns off interim user accounting when no value is specified in the RADIUS Acct-Interim-Interval attribute.

Related Documentation

- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- Service Interim Accounting Overview on page 24
- Service Interim Accounting for IPv4 and IPv6 Services in a Dual Stack Overview on page 27
- **aaa service accounting interval on page 112**
- **aaa user accounting interval on page 113**

Configuring Calculation of Service Session Accounting Based on Scheduler Profiles Instead of Rate-Limit Profiles in Hierarchical Parent Groups for Forwarded Packets

You can configure the Service Manager application to compute accounting for service sessions based on the number of packets that are forwarded by the scheduler profile in QoS profiles on output interfaces. Service Manager collects statistics from parent groups that are configured in an output policy attached to an interface. Each parent group might contain a rate-limit profile. When packets enter an interface to which a rate-limit profile

is applied, the router counts the number of bytes (packets) over time, categorizes each packet as committed, conformed, or exceeded, and assigns a transmit, drop, or mark action to the packets.

Parent groups configured in a hierarchy are effectively used in a layer 2 (ATM) access network for digital subscriber lines (DSLs) where many routing gateways lead to one Broadband Remote Access Server (B-RAS). The B-RAS uses rate-limit hierarchies to allocate shareable bandwidth to each routing gateway, which enables unused bandwidth from one routing gateway to be used by others.

Each rate-limit profile in a hierarchical parent group processes and classifies the packets that arrive at an interface, and computes the statistics to be displayed in the output of the **show** commands for the relevant interfaces. For rate-limit profiles in a hierarchical parent group that are part of classifier groups in a policy attached to an output interface, if you configure a scheduler profile in a QoS profile and attach it to the same output interface, the packets processed by the rate-limit profile in the hierarchical parent group might be either forwarded or dropped based on the scheduler profile attached to the interface. A scheduler profile configures the bandwidth at which a traffic queue is validated as a function of relative weight, assured rate, and shaping rate.

This method of operation causes discrepancies and inaccuracies in the accounting statistics for subscriber service sessions that the Service Manager application collects. Because packets that are treated as forwarded packets at the rate-limit profile in a hierarchical parent group might be classified in a different way at some other level in a rate-limit hierarchy, incorrect accounting statistics are retrieved for service sessions.

In an environment in which you apply policies, with rate-limit profiles defined in a hierarchical parent group, to interfaces that are also assigned with scheduler profiles, you can enable Service Manager to calculate accounting information for subscriber sessions based on the packets forwarded by scheduler profiles. You can use the **service-accounting-statistics scheduler-based** command in Global Configuration mode to enable this capability to compute accounting details based on scheduler profiles for policies with hierarchical rate-limit profiles on output interfaces. By default, this feature is not enabled. This functionality is effective only for packets that are forwarded at an output interface by a policy that contains a rate-limit profile in a hierarchical parent group and does not apply to packets that are dropped by the rate-limit profile.

When you enable or disable this feature, the statistical values collected for policies that contain rate-limit profiles in hierarchical parent groups on output interfaces are reset. This setting to calculate accounting details for service sessions based on scheduler profiles is preserved across an upgrade operation.

When you enable this functionality, the following operations are performed:

- The packet received at an output interface is processed by the rate-limit profile defined in a hierarchical parent group after classification. If the packet is marked to be transmitted based on the action specified in the rate-limit profile, the statistical counter to save the number of forwarded packets in the parent group is not incremented. When the packet arrives at the scheduler profile and is processed by it, if it is scheduled to be forwarded, the counter to store the number of forwarded packets for each rate-limit profile is incremented.

- If the incoming packet is determined to be dropped by the rate-limit profile in the parent group against which it is validated, the counter to record the number of dropped packets of the parent group is incremented.

If you enable scheduler profile–based computation of service session accounting, for IPv4, IPv6, or MPLS interfaces, the output of the **show ip interface** , **show ipv6 interface**, or **show mpls interface** commands display the forwarded packets and bytes fields, and dropped packets and bytes fields in the rate-limit-profile section under the IP, IPv6, or MPLS policy output headings for policies with hierarchical parent groups. The committed, conformed, exceeded, saturated, and unconditional packets and bytes fields are not displayed in the rate-limit-profile section in the output of these commands for policies with hierarchical parent groups.

To enable computation of accounting statistics for service sessions based on scheduler profiles for forwarded packets with rate-limit profiles in hierarchical parent groups on output interfaces:

- From Global Configuration mode, enable the capability to calculate accounting statistics for subscriber service sessions by using scheduler profiles instead of rate-limit profiles in hierarchical parent groups:

  host1(config)#service-accounting-statistics scheduler-based

  Use the **no** version of this command to disable the computation of accounting details based on scheduler profiles. In such a case, the accounting information is computed based on rate-limit profiles defined in hierarchical parent groups for policies on output interfaces.

Related Documentation

- Verifying Computation of Service Session Accounting Based on Scheduler Profiles on page 143
- service-accounting-statistics scheduler-based
- show service-accounting-statistics

CHAPTER 16

Configuration Task for Service Session Profiles

Using Service Session Profiles to Deactivate Service Sessions

To terminate a subscriber service session when a threshold is reached, you create a service session profile that includes a time threshold, or a volume threshold, or both. Then, you attach the service session profile when you activate the service session. When the specified threshold is reached, the service session is terminated.

NOTE: This feature is not supported by the **service-management owner-session** command. The **service-management owner-session** command only supports service session profiles when activating service sessions.

The following procedure shows the commands you might use to create a time threshold for deactivating a service session. See "Working with Service Session Profiles" on page 68 for information about using the **time** and **volume** keywords in service session profiles.

To create or modify a service session profile:

1. Specify the name of the service session profile and configure the threshold:

   ```
   host1(config)#service-management service-session-profile vodISP1
   host1(config-service-session-profile)#time 6000
   host1(config-service-session-profile)#exit
   ```

2. Include the service session profile when you activate the subscriber service session:

   ```
   host1(config)#service-management subscriber-session client1@isp1.com  interface
     atm 4/0.1 service-session "video(4500000, 192.168.10.3)"  service-session-profile
     vodISP1
   ```

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68

- Activating Subscriber Sessions Using the CLI on page 51
- Preprovisioning Service Sessions on page 53
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18
- Gracefully Deactivating Subscriber Service Sessions on page 54
- Forcing Immediate Deactivation of Subscriber Service Sessions on page 55
- **service-management owner-session on page 131**
- **service-management subscriber-session service-session on page 132**

Working with Service Session Profiles

This topic describes the settings you can configure for a new service session profile or the attributes you can modify in an existing service session profile. Creating or modifying a service session profile comprises the following sets of tasks:

NOTE: To modify an existing profile, you can add new attributes or use the **no** version of a command to remove an attribute.

- Creating a New Service Session Profile on page 68
- Specifying Statistics Collection Settings on page 69
- Specifying the Maximum Bandwidth for a Service Session on page 69
- Specifying the Interval for the Active State of a Service Session on page 70

Creating a New Service Session Profile

You can create a new service session profile, and enter Service Session Profile Configuration mode by using the **service-management service-session-profile** command. You can also use this command to modify the attributes of a previously created profile.

To create a new service session profile:

- Issue the **service-management service-session-profile** command in Global Configuration mode. Issuing this command enables you to access Service Session Profile Configuration mode.

  ```
  host1(config)#service-management service-session-profile vodISP1
  host1(config-service-session-profile)#
  ```

  In Service Session Profile Configuration mode, you specify the attributes used in the service session profile, such as the maximum volume limit for the session and the maximum time the session can be used. You can also specify that Service Manager collect statistics for time, or volume, or both.

  Use the **no** version to delete the service session profile.

Specifying Statistics Collection Settings

You can use the **statistics** command in Service Session Profile Configuration mode to enable statistics collection and to specify the type of statistics to collect.

- Use the **time** keyword with the **statistics** command to collect statistics about the duration of the service session.

  ```
  host1(config)#service-management service-session-profile vodISP1
  host1(config-service-session-profile)#statistics time
  ```

- Use the **volume-time** keyword with the **statistics** command to collect statistics about both the volume of traffic and the duration of the service session.

  ```
  host1(config)#service-management service-session-profile vodISP1
  host1(config-service-session-profile)#statistics volume-time
  ```

  Use the **no** version to disable statistics collection.

NOTE: Service Manager statistics collection is a three-part procedure. You must configure statistics information in the service definition macro file, enable statistics collection by either RADIUS or the CLI, and also enable statistics collection for the policy referenced in the service macro using the **statistics enabled** keyword in the command used for policy attachment in the profile. See "Configuring Service Manager Statistics" on page 71.

Specifying the Maximum Bandwidth for a Service Session

You can use the **volume** command in Service Session Profile configuration mode to specify the maximum amount of bandwidth that can use the service.

To configure the maximum amount of bandwidth for a service session:

- Issue the **volume** command in Service Session Profile configuration mode.

  ```
  host1(config)#service-management service-session-profile vodISP1
  host1(config-service-session-profile)#volume 1000000
  ```

The router immediately terminates the subscriber's service session when the specified traffic volume is exceeded. The range is 0–16777251MB.

Use the **no** version to delete the volume attribute from the service session profile.

NOTE: The **volume** attribute uses values captured by the Service Manager statistics feature to determine when the threshold is exceeded. Therefore, you must configure and enable statistics collection to use this attribute. See "Configuring Service Manager Statistics" on page 71.

Specifying the Interval for the Active State of a Service Session

You can use the **time** command in Service Session Profile configuration mode to specify the maximum amount of time that the service session can be active for the subscriber.

To configure the maximum duration for which a subscriber service session can be active:

- Issue the **time** command in Service Session Profile configuration mode.

  ```
  host1(config)#service-management service-session-profile vodISP1
  host1(config-service-session-profile)#time 6000
  ```

  The router immediately terminates the subscriber's service session when the specified time is exceeded. The range is 0–16777251 seconds.

  Use the **no** version to delete the time attribute from the service session profile.

Related Documentation

- Service Session Profiles Overview on page 29
- Activating Subscriber Sessions Using the CLI on page 51
- Overview of Deactivating Subscriber Service Sessions Using the CLI on page 18
- Preprovisioning Service Sessions on page 53
- Gracefully Deactivating Subscriber Service Sessions on page 54
- Forcing Immediate Deactivation of Subscriber Service Sessions on page 55
- Using Service Session Profiles to Deactivate Service Sessions on page 67
- **service-management service-session-profile on page 130**
- **statistics on page 133**
- **time on page 134**
- **volume on page 135**

CHAPTER 17

Configuration Task for Service Manager Statistics

Configuring Service Manager Statistics

The Service Manager application provides a flexible and efficient process for identifying and capturing statistics related to subscriber service sessions. Configuring Service Manager to collect statistics is a three- part process. First, you design the service definition macro file to identify the statistics that you want to collect. Second, you configure Service Manager to enable statistics collection when a service session is activated by either RADIUS or the CLI. Third, before you reference a policy in the service definition macro to enable Service Manager collect statistics, you must enable statistics collection for this policy using the **statistics enabled** keyword in the command used for policy attachment in the profile.

The following topics describe how to configure the service definition macro file. For information about configuring Service Manager to enable statistics, see the *Enabling Statistics Collection with the CLI* section if you are using RADIUS to activate services, or see *Enabling Statistics Collection with RADIUS* section if you are using the CLI.

Configuring Service Manager statistics involves the following sets of tasks:

Setting Up the Service Definition File for Statistics Collection

Service Manager statistics are based on classifier lists—the classifier lists are referenced by policy lists that you define in your service definition macro file.

When you configure your service definition for statistics, you include the macro environment command **env.setResult** to indicate the type of statistics to track and to identify the classifier lists to use when generating statistics. The format of the environment command is:

```
<# env.setResult(“string” , “classifier-list-name” ) #>
```

The *string* variable specifies the type of statistics to track—Service Manager supports the following strings:

- **input-stat-clacl**—track input statistics
- **output-stat-clacl**—track output statistics
- **secondary-input-stat-clacl**—track input statistics for a policy attached at the secondary input stage

The *classifier-list-name* variable is the name of the classifier list that is associated with the policy list that is defined in the service definition. You can specify multiple classifier lists in the command.

This example is a portion of the service definition macro file in “Creating Service Definitions” on page 41. The two highlighted commands specify the statistics used by the Service Manager application.

```
profile <# name; '\n' #>
    ip policy secondary-input <# name #> statistics enabled merge
    ip policy output <# oname #> statistics enabled merge
    qos-profile triplePlayIP
    qos-parameter maxSubscBW <# outputBW; '\n' #>
   <# env.setResult("activate-profile", name) #> <#
   env.setResult("secondary-input-stat-clacl", "matchAll") #> <#
   env.setResult("output-stat-clacl", "matchAll") #>
   <# endtmpl #>
```

The **<# env.setResult("secondary-input-stat-clacl", "matchAll") #>** command specifies that Service Manager track statistics associated with the classifier list named matchAll, and that this classifier list is associated with the policy that is attached at the secondary input stage.

The **<# env.setResult("output-stat-clacl", "matchAll") #>** command specifies that Service Manager track the output statistics associated with the matchAll classifier list, which is associated with the policy attached at the output stage.

NOTE: Before you reference as policy in the service definition macro to enable Service Manager collect statistics, you must enable statistics collection for this policy using the **statistics enabled** keyword in the command used for policy attachment in the profile.

This example shows how you can also configure your service definition to collect total statistics from multiple classifier lists. The following command specifies that three classifier lists are used to generate output statistics for a service created by the service definition. Each time statistics are reported for this service, Service Manager uses the total of the statistics for clacl1, clacl2, and clacl3.

```
<# env.setResult("output-stat-clacl", "clacl1 clacl2 clacl3” ) #>
```

Enabling Statistics Collection with RADIUS

You use the Service-Statistics RADIUS VSA [26-69] with either the RADIUS login or CoA-Request method to enable statistics for RADIUS-activated service sessions. To enable statistics, configure the Service-Statistics VSA with a value of either 1 (timestamp only) or 2 (volume and timestamp).

Table 10 on page 73 describes a partial RADIUS message in which the Service-Statistics attribute has a value of 2—this enables volume and timestamp statistics for the tiered service assigned to subscriber client1@isp1.com.

Table 10: RADIUS-Enabled Statistics

RADIUS Attribute	Tag	Value
username	none	client1@isp1.com
activate-service	6	tiered(1280000, 5120000)
service-statistics	6	2

When you enable statistics for a RADIUS-activated service, RADIUS accounting reports can use the statistics.

Enabling Statistics Collection with the CLI

You use service session profiles to enable statistics when you activate a service session with the CLI. See "Service Session Profiles Overview" on page 29 for detailed information about creating and using service session profiles.

For example, you can use the following procedure to capture statistics that are defined in the service definition macro file for the tiered service:

1. Configure the service session profile to enable statistics. Specify the type of statistics you want to capture (either time or both volume and time).

   host1(config)#service-management service-session-profile isp1_tiered3
   host1(config-service-session-profile)#statistics volume-time
   host1(config-service-session-profile)#

2. Apply the service session when you activate the subscriber service session.

   host1(config)#service-management subscriber-session client1@isp1.com interface atm 4/0.1 service-session " tiered(1000000, 2000000)" service-session-profile isp1_tiered3

The captured statistics are now used when you use the Service Manager **show service-management** commands. For example:

```
host1# show service-management subscriber-session client1@isp1.com interface atm 4/0.1
service-session
User Name: client1@isp1.com, Interface: atm 4/0.1
Service : tiered(1000000,2000000)
 Non-volatile : False
 Owner : CLI
```

```
State : Config ApplySuccess
Activate : True
Statistics Type : time-based and volume-based
Statistics Complete : False
Poll Interval : 0
Poll Expire : 0
Activate Time : THU MAR 01 21:09:12 2006
Time : 0
Time Expire : 0
Volume MBytes: 2
Volume Expire MBytes: 1
Input Bytes : 594
Output Bytes : 1196
Input Packets : 1
Output Packets : 2
```

Setting Up the External Parent Group Statistics Collection

Policies for interface groups include external parent groups that are implicitly instantiated during policy attachment based on each unique interface group encountered. You can use external parent groups and policy parameters for sharing aggregate nodes across policy attachments. Each external parent group reference in a policy is accompanied by a parameter that is resolved during the attachment of the policy to an interface.

You can retrieve either external parent group statistics or classifier statistics from policy manager. However, you cannot retrieve both statistics for a single service definition. When a combined service is configured, you cannot retrieve classifier list-based based statistics. In such a scenario, you can only retrieve external parent group-based statistics from policy manager.

Only hierarchical policy parameters can have external parent group references. Each parameter has a single value, depending on the type of parameter. The hierarchical policy parameter can have a single numeric value or a keyword. When you configure your service definition for statistics, you include the macro environment command env.setResult to indicate the type of statistics to track and to identify the external parent groups to use when generating statistics. The format of the environment command is:

<# env.setResult("*string*" , "*external-parent-grp-name policy-parameter-name*") #>

The *string* variable specifies the type of statistics to track. Service Manager supports the following strings:

- **input-stat-epg**—Track input statistics for an external parent group in a hierarchical policy
- **output-stat-epg**—Track output statistics for an external parent group in a hierarchical policy
- **secondary-input-stat-epg**—Track input statistics for an external parent group in a hierarchical policy attached at the secondary input stage

The *external-parent-grp-name* variable is the name of the external parent group that a classifier group refers to in the policy list that is defined in the service definition. You must specify the external parent group and the hierarchical policy in the env.setResult command as a pair. You can specify multiple pairs of external parent groups and hierarchical policies

in the command. The *policy-parameter-name* variable is the name of the hierarchical policy that allows classifier groups and parent groups within a policy to point to line module global parent groups. Each reference to a policy parameter in a policy is substituted with its value for all attachments of this policy at the interface.

For example, if *v4v6* is the name of the hierarchical policy parameter and the external parent group names are *vc-v4v6-in* and *vc-v4v6-out*, you must configure both the external parent group names and the corresponding hierarchical policy parameter in the env.setResult method for the external parent group statistics to be calculated.

```
<# env.setResult("input-stat-epg", "vc-v4v6-in v4v6" ) #>
<# env.setResult("output-stat-epg", "vc-v4v6-out v4v6" ) #>
```

The **<# env.setResult("secondary-input-stat-epg", "vc-v4v6-in v4v6") #>** command specifies that Service Manager track statistics associated with the external parent group named vc-v4v6-in and the corresponding hierarchical policy named v4v6, and that this external parent group is associated with the policy that is attached at the input stage.

The **<# env.setResult("output-stat-epg", "vc-v4v6-out v4v6") #>** command specifies that Service Manager track the output statistics associated with the external parent group named vc-v4v6-out and the corresponding hierarchical policy named v4v6, which is associated with the policy attached at the output stage.

The input and output statistics associated with the external parent group are collected and forwarded to the Service Manager to be displayed in the Acct-Stop and Interim-Acct messages.

Related Documentation

- Service Session Profiles Overview on page 29
- Working with Service Session Profiles on page 68
- Service Definitions Overview on page 9
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- **service-management service-session-profile on page 130**
- **service-management subscriber-session service-session on page 132**
- **show service-management service-session-profile on page 178**

CHAPTER 18

Working with QoS Configurations for Service Manager

Referencing QoS Configurations in Service Definitions

You can use QoS profiles and QoS parameters to define a service for a subscriber. For example, you can configure the shaping rate for traffic in a video service by using a QoS parameter instance.

To transmit the QoS configuration to the subscriber interface (that is, the forwarding interface at the top of the interface column), you must configure the QoS profiles and QoS parameter instances in static profiles.

To reference QoS configurations in service definitions, perform the following tasks:

- Specifying QoS Profiles in Service Definitions on page 78
- Specifying QoS Parameter Instances in a Service Definition on page 79

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Overview of Referencing Policies in Service Definitions on page 8
- Modifying QoS Configurations with Service Manager on page 81
- Removing QoS Configurations Referenced by Service Manager on page 84
- Specifying QoS Profiles in Service Definitions on page 78
- QoS for Service Manager Considerations on page 7

Specifying QoS Profiles in Service Definitions

You can configure one QoS profile per subscriber interface. We recommend that you specify the QoS profile in the first set of services applied to the subscriber's interface.

You can modify the QoS profile by modifying configurations referenced by the QoS profile, including QoS parameter instances. You can also attach a new QoS profile when activating a service, but make sure that the QoS profile is attached to the subscriber's interface.

For more information about configuring QoS profiles, see the *Configuring and Attaching QoS Profiles to an Interface* chapter in *JunosE Quality of Service Configuration Guide*.

To reference QoS profiles in a service definition, perform the following tasks:

- Configuring a QoS Profile for Service Manager on page 78
- Specifying QoS Profiles in a Service Definition on page 78

Configuring a QoS Profile for Service Manager

To configure a QoS profile for Service Manager:

1. Configure the profile.

   ```
   host1(config)#profile videoService
   host1(config-profile)#
   ```

   When you specify the name of the profile to be configured, you enter Profile Configuration mode. You can specify a profile name with up to 80 alphanumeric characters.

   Use the **no** version to remove a profile.

2. Configure the QoS profile.

   ```
   host1(config-profile)#qos-profile videoBandwidth1
   ```

   You can use this command to create a QoS profile on the router for use with Service Manager and enter QoS Profile Configuration mode. When the service is activated, the QoS profile is created and attached to the subscriber interface.

   Use the **no** version to remove the QoS profile from the profile.

3. (Optional) Complete the QoS profile configuration described in the *Configuring and Attaching QoS Profiles to an Interface* chapter in *JunosE Quality of Service Configuration Guide*.

Specifying QoS Profiles in a Service Definition

After you configure a QoS profile for Service Manager, you can reference it in a service definition. For example:

```
profile <# eastcoast ; '\n' #>
qos-profile <# video; '\n' #>
```

In this example, activating the service definition attaches the video QoS profile to the subscriber interface. Service Manager overwrites the existing QoS profile attachment at the subscriber interface.

Deactivating the service detaches the video QoS profile from the subscriber interface.

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Referencing QoS Configurations in Service Definitions on page 77
- Modifying QoS Configurations with Service Manager on page 81
- Removing QoS Configurations Referenced by Service Manager on page 84
- **profile on page 127**
- **qos-profile on page 128**

Specifying QoS Parameter Instances in a Service Definition

You can specify that Service Manager create QoS parameter instances when the subscriber logs in (during service activation) or through RADIUS QoS parameter VSAs.

You can specify up to eight parameter instance commands within a profile. When you activate a service, Service Manager creates or modifies parameter instances for the subscriber interface that matches one of the subscriber-interface types configured in the QoS parameter definition.

Deactivating a service can modify or remove QoS parameter instances.

Using a service definition, you can also configure QoS parameters instances to add value to an existing parameter instance using the **add** keyword or dynamically create new parameter instances with an initial value using the **initial-value** keyword.

For more information about configuring QoS parameters, see *JunosE Quality of Service Configuration Guide*, QoS Parameter Overview.

To specify QoS parameter instances in a service definition, perform the following tasks:

- Creating a Parameter Instance in a Profile on page 79
- Specifying QoS Parameter Instances in a Service Definition on page 80

Creating a Parameter Instance in a Profile

To create a QoS parameter instance for Service Manager:

1. Configure the QoS parameter definition described in *JunosE Quality of Service Configuration Guide*, QoS Parameter Overview.

   You must configure at least one controlled-interface type and one subscriber-interface type. The range specified in the parameter definition controls the available value of the parameter instance.

2. Configure the QoS profile.

   host1(config)#profile video

3. Configure the QoS parameter instance command in the profile.

   host1(config-profile)#qos-parameter videoBandwidth1 add 40000

   When the service is activated, the parameter instances are created for the subscriber interface.

   You can use the **add** keyword with this command in Profile Configuration mode to add a value to an existing parameter instance.

   You can use the **initial-value** keyword with this command to create a new instance with the specified value.

   host1(config-profile)#qos-parameter max-subscriber-bandwidth initial-value 15000

   Use the **no** version to remove the QoS parameter instance command in the profile.

Specifying QoS Parameter Instances in a Service Definition

After you configure a QoS parameter instance for Service Manager, you can reference it in a service definition. For example:

```
<# qosserviceone(bandwidth1, bandwidth2) #>
profile <# profileName ; '\n' #>
qos-parameter <# qosParameterName1 ; ' ' ; bandwidth1 ; '\n' #>
qos-parameter <# qosParameterName2 ; ' ' ; bandwidth2 ; '\n' #>
<# endtmpl #>
```

When you activate a service, Service Manager creates the parameter instance and overwrites previous parameter instances. For example, activating the qosserviceone service definition creates a profile containing two QoS parameter instances. Service Manager creates the qosParameterName1 parameter instance with the value of bandwidth1, and creates qosParameterName2 with a value of bandwidth2.

If you activate the service definition using qosserviceone(2000000,3000000), Service Manager creates qosParameterName1 with a value of 2000000 and qosParameterName2 instance with a value of 3000000.

You can use the **add** keyword to add value to an existing parameter instance. For example:

```
<# qosserviceone(bandwidth1, bandwidth2) #>
profile <# profileName ; '\n' #>
qos-parameter <# qosParameterName3 ; ' add ' ; bandwidth2 ; '\n' #>


<# endtmpl #>
```

When you specify parameter instances using the **add** keyword, you can also use the **initial-value** keyword to specify an initial value. For example:

```
<# qosserviceone(bandwidth1, bandwidth2) #>
profile <# profileName ; '\n' #>
qos-parameter <# qosParameterName4 ; ' add ' ; bandwidth2 ;
' initial-value 1000000' ; '\n' #>
```

```
<# endtmpl #>
```

When you activate the service, Service Manager locates the existing QoS parameter instance in the interface column. If Service Manager does not find a parameter instance, it creates one with a value specified in the **initial-value** keyword (in this case, 100000). The value in the command is then added to the initial value. If an existing parameter instance is found, Service Manager adds the value to the existing interface.

For example, when you activate qosServiceOne as qosServiceOne(2000000,3000000), Service Manager attempts to locate the parameter instance qosParameterName4 for the subscriber's interface. If it finds a parameter instance, it adds bandwidth2 (3,000,000) to the current value. If Service Manager does not find a parameter instance, it creates one with an initial value of 1,000,000 and adds 3,000,000. The final parameter instance value is 4,000,000.

When deactivating the service, Service Manager locates the QoS parameter instance and subtracts the value in the command from the existing instance value. If the parameter is no longer referenced, the parameter instance is removed.

Related Documentation

- Modifying QoS Configurations with Service Manager on page 81
- Removing QoS Configurations Referenced by Service Manager on page 84

Modifying QoS Configurations with Service Manager

This topic describes how to modify QoS configurations with Service Manager. To modify QoS configurations with Service Manager, perform the following steps:

- Modifying Parameter Instances on page 81
- Modifying QoS Configurations in a Single Service Manager Event on page 83
- Modifying QoS Configurations Using Other Sources on page 83

Modifying Parameter Instances

Service Manager activates services without considering current parameter instance values. For example, when you deactivate a video service, Service Manager can add 5 Mbps to a parameter associated with the shaping rate of a video queue.

Similarly, Service Manager can deactivate services and restore parameter instances to their previous value. For example, when you deactivate a video service, Service Manager can subtract 5 Mbps from a parameter associated with the shaping rate of a video queue.

Table 11 on page 81 lists the results of a series of activations and deactivations of parameters using the **add** and **initial-value** keywords.

Table 11: Sample Modifications Using the Add and Initial-Value Keywords

Action	QoS Parameter Instance	Result
Activate	qos-parameter video-bw add 5000000 initial-value 0	Parameter instance video-bw is created with a value of 5000000

Table 11: Sample Modifications Using the Add and Initial-Value Keywords *(continued)*

Action	QoS Parameter Instance	Result
Activate	qos-parameter video-bw add 1000000 initial-value 0	Parameter instance video-bw is increased by 1000000, for a total of 6000000
Deactivate	qos-parameter video-bw add 1000000 initial-value 0	Parameter instance video-bw is decreased by 1000000, for a total of 500000
Deactivate	qos-parameter video-bw add 5000000 initial-value 0	Parameter instance video-bw is removed

Removing a parameter instance using profiles is based on the number of times a parameter instance is modified, not the value added.

Modifying parameter instances in profiles and modifying explicit parameter instances can cause invalid parameter instance values. Table 12 on page 82 lists a series of activations and deactivations using parameter instances in profiles and explicit parameter instances. By the second deactivation, the parameter has a negative value (-4000000).

NOTE: We recommend that you do not configure negative values for Service Manager.

Table 12: Sample Modifications Using Parameter Instances

Action	QoS Parameter Instance	Result
Activate	qos-parameter video-bw add 5000000 initial-value 0	Parameter instance video-bw is created with a value of 5000000
Activate	qos-parameter video-bw add 1000000 initial-value 0	1000000 is added to parameter instance video-bw, for a total of 6000000
Activate	qos-parameter video-bw 2000000	Parameter instance video-bw is set to 2000000
Deactivate	qos-parameter video-bw add 1000000 initial-value 0	1000000 is subtracted from parameter instance video-bw for a total of 1000000
Deactivate	qos-parameter video-bw add 5000000 initial-value 0	5000000 is subtracted from parameter instance video-bw for a total of -4000000
Deactivate	qos-parameter video-bw 2000000	Parameter instance video-bw is removed

Modifying QoS Configurations in a Single Service Manager Event

QoS accepts QoS profile attachments and parameter instances created using multiple sources (profiles, RADIUS, or Service Manager) within a single Service Manager event. Events include:

- Subscriber login
- Subscriber logout
- RADIUS Change of Authority (CoA)

QoS prioritizes the creation of QoS profiles and parameter instances within events. Table 13 on page 83 lists the sources that overwrite QoS profiles and parameter instances created by other sources. Each row represents new QoS profiles and parameter instances; columns represent existing QoS profiles and parameter instances.

Table 13: Configuration Within a Single Service Manager Event

	Profile	RADIUS	Service Manager
Profile	✓	–	–
RADIUS	✓	✓	–
Service Manager	✓	✓	✓

Modifying QoS Configurations Using Other Sources

You can modify QoS configurations with Service Manager by using other QoS sources. For example, you can modify a parameter instance that was created with Service Manager by using the CLI. Similarly, you can use SNMP to detach a QoS profile attached by Service Manager.

Table 14 on page 83 lists the sources that you can use to modify QoS profile attachments and parameter instances.

Table 14: Modifying QoS Configurations with Other Sources

	QoS Profile Attachment	QoS Parameter Instances
Service Manager	✓	✓
RADIUS	✓	✓
SNMP	✓	–
SRC software	✓	–
CLI	✓	✓

The following sections describe the precedence of each source when modifying configurations.

Service Manager

QoS profile attachments and parameter instances created through Service Manager have precedence over all other sources. For example, Service Manager can overwrite a QoS profile attachment modified through RADIUS, SNMP, the SRC software, or the CLI.

Conversely, Service Manager configurations can be overwritten through SNMP, the SRC software, and the CLI, but not by RADIUS.

Service Manager counts references of parameter instances. You can modify parameter instances created by Service Manager using other sources without affecting the reference counts. For more information, see "QoS for Service Manager Considerations" on page 7.

RADIUS

QoS profile attachments and parameter instances configured through RADIUS can overwrite QoS profile attachments and parameter instances configured through the SNMP, the SRC software, and the CLI, but not those created by Service Manager.

Conversely, QoS profiles and parameter instances configured through RADIUS can be overwritten by any source (SNMP, the SRC software, CLI, and Service Manager).

SNMP, the SRC Software, and the CLI

QoS profile attachments and parameter instances configured through the CLI can overwrite QoS profile attachments and parameter instances configured through any source.

QoS profiles attached through SNMP and the SRC software can also overwrite QoS profile attachments configured through any source.

Conversely, QoS profiles and parameter instances configured through the CLI, SNMP, or the SRC software can be overwritten by any source.

Related Documentation

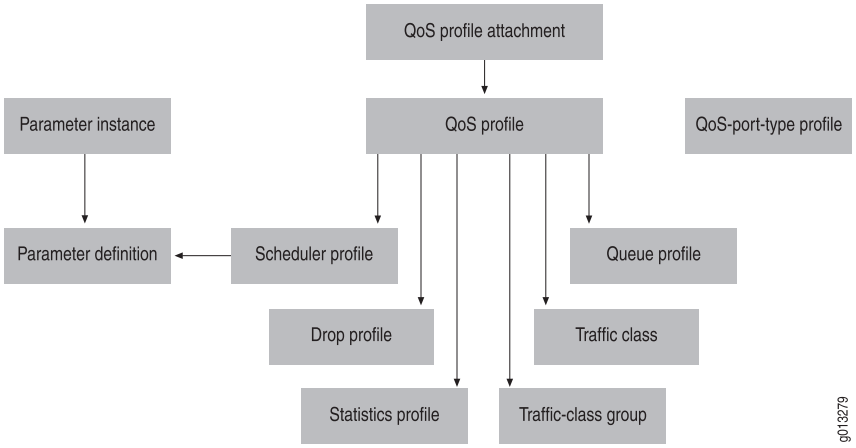
- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Specifying QoS Profiles in Service Definitions on page 78
- Referencing QoS Configurations in Service Definitions on page 77
- Removing QoS Configurations Referenced by Service Manager on page 84
- QoS for Service Manager Considerations on page 7

Removing QoS Configurations Referenced by Service Manager

When Service Manager no longer references a QoS configuration, it must be removed from the service definition.

Figure 4 on page 85 shows the references for QoS configurations.

Figure 4: QoS Configuration Dependency Chain



Service Manager automatically removes QoS profiles and parameter instances. After removing the QoS profile and parameter instances, Service Manager automatically removes the following QoS configurations in the following order:

1. QoS profiles
2. Scheduler profiles
3. Queue profiles
4. Drop profiles
5. Statistics profiles

Service Manager does not automatically remove the following QoS configurations:

- Parameter definitions
- Traffic classes
- Traffic-class groups
- QoS-port-type profiles

Related Documentation

- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Specifying QoS Profiles in Service Definitions on page 78
- Referencing QoS Configurations in Service Definitions on page 77
- Modifying QoS Configurations with Service Manager on page 81
- QoS for Service Manager Considerations on page 7

CHAPTER 19

Configuration Tasks for HTTP Local Server for Guided Entrance

Configuring the HTTP Local Server to Support Guided Entrance

JunosE Software supports an embedded Web server, known as the HTTP local server, which is used to support the Service Manager application's guided entrance service. With guided entrance, subscribers are directed to a specific Web site when they log in. At the Web site, the subscribers can then select the service they want to use. You can configure one HTTP local server per virtual router. The HTTP local server is disabled by default.

In lower-numbered releases, the HTTP server listened for and processed only IPv4 exception packets. You can now configure the HTTP local server to listen for and process both IPv4 and IPv6 packets.

NOTE: **Currently, the HTTP local server does not support two different ports for IPv4 and IPv6 packets. However, the HTTP local server can listen for both IPv4 and IPv6 exception packets on the same port, simultaneously.**

The following topics explain how to configure the HTTP local server to support guided entrance:

Configuring the HTTP Local Server to Support Guided Entrance for IPv4 Subscribers

To configure the HTTP local server to support guided entrance for IPv4:

1. Access the virtual router context.

   ```
   host1(config)#virtual-router west400
   host1:west400(config)#
   ```

2. Create the HTTP local server.

   ```
   host1:west40(config)#ip http
   ```

   Use the **no** version to delete the HTTP local server.

3. (Optional) Specify a standard IP access list that defines which subscribers can connect to the HTTP local server.

   ```
   host1:west40(config)#ip http access-class chicagoList
   ```

   Use the **no** version to remove the association between the access list and the HTTP local server.

4. (Optional) Specify the port on which the HTTP local server receives connection attempts.

   ```
   host1:west40(config)#ip http port 8080
   ```

   You can specify a port number in the range 1–65535. Use the **no** version to restore the default port number, 80.

5. (Optional) Specify the maximum number of connections that can exist between one IP address and the HTTP local server.

   ```
   host1:west40(config)#ip http same-host-limit 20
   ```

   You can specify a number in the range 0–1000.

   Use the **no** version to restore the default number of allowed connections, 3.

6. Specify the maximum time that HTTP local servers maintain connections.

   ```
   host1:west40(config)#ip http max-connection-time 1000
   ```

   You can specify a time in the range 3–7200 seconds, or 0. A value of 0 causes the server to maintain an inactive connection indefinitely. Use the **no** version to restore the default time, 30 seconds.

7. Enable the HTTP local server to listen for and process IPv4 exception packets

   ```
   host1:west40(config)#ip http server
   ```

   Use the **no** version to disable the HTTP local server.

8. Configure the HTTP redirect feature for the profile, interface, or subinterface that will be referenced in the guided entrance service definition.

   ```
   host1:west40(config)#profile guidEnt6
   host1:west40(config-profile)#ip http redirectUrl http://ispsite.redirect.com
   ```

   The first access session is typically used by the Service Manager application to provide initial provisioning and service selection for the subscriber. HTTP redirect is per-interface; use the command in Profile Configuration mode for dynamic interfaces; use the command in Interface Configuration mode or Subinterface Configuration mode for static interfaces.

   The redirect URL can be a maximum of 230 characters.

NOTE: The HTTP local server must be configured and enabled in the virtual router for the interface on which you use the **ip http redirectUrl** command. Otherwise, the URL redirect operation will fail.

Use the **no** version to restore the default, which disables the HTTP redirect feature.

Configuring the HTTP Local Server to Support Guided Entrance for IPv6 Subscribers

To configure the HTTP local server to support guided entrance for IPv6:

1. Access the virtual router context.

   ```
   host1(config)#virtual-router west400
   host1:west400(config)#
   ```

2. Create the HTTP local server.

   ```
   host1:west40(config)#ipv6 http
   ```

   Use the **no** version to delete the HTTP local server.

3. (Optional) Specify a standard IP access list that defines which subscribers can connect to the HTTP local server.

   ```
   host1:west40(config)#ip http access-class chicagoList
   ```

   Use the **no** version to remove the association between the access list and the HTTP local server.

4. (Optional) Specify the port on which the HTTP local server receives connection attempts.

   ```
   host1:west40(config)#ipv6 http port 8080
   ```

   NOTE: You can modify the port on which the HTTP local server receives connection attempts. However, you must first disable the HTTP local server and then modify the port.

   You can specify a port number in the range 1–65535. Use the **no** version to restore the default port number, 80.

5. (Optional) Specify the maximum number of connections that can exist between one IP address and the HTTP local server.

   ```
   host1:west40(config)#ip http same-host-limit 20
   ```

   You can specify a number in the range 0–1000. Use the **no** version to restore the default number of allowed connections, 3.

6. Specify the maximum time that HTTP local servers maintain connections.

   ```
   host1:west40(config)#ip http max-connection-time 1000
   ```

You can specify a time in the range 3–7200 seconds, or 0. A value of 0 causes the server to maintain an inactive connection indefinitely. Use the **no** version to restore the default time, 30 seconds.

7. Enable the HTTP local server to listen for and process IPv6 exception packets.

   ```
   host1:west40(config)#ipv6 http server
   ```

   Use the **no** version to disable the HTTP local server.

8. Configure the HTTP redirect feature for the IPv6 profile, interface or subinterface to be referenced in the guided entrance service definition.

   ```
   host1:west40(config)#interface gigabitEthernet 6/0
   host1:west40(config-if)#ipv6 http redirectUrl http://ispsite.redirect.com
   ```

   The first access session is typically used by the Service Manager application to provide initial provisioning and service selection for the subscriber. HTTP redirect is per-interface; use the command in Interface Configuration mode or Subinterface Configuration mode for static interfaces and use the command in Profile Configuration mode for dynamic interfaces.

   The redirect URL can be a maximum of 230 characters.

   NOTE: The HTTP local server must be configured and enabled in the virtual router for the interface on which you use the **ipv6 http redirectUrl** command. Otherwise, the URL redirect operation will fail.

   Use the **no** version to restore the default, which disables the HTTP redirect feature.

Related Documentation

- Guided Entrance Service Overview on page 31
- Using CoA Messages with Guided Entrance Services on page 91
- Example: Guided Entrance Service Definition on page 101
- Redirection of Subscriber Sessions When HTTP Local Server is Disabled or Not Configured on page 32
- Configuring the Preservation of the Original URL During Redirection of Subscriber Sessions on page 92
- **ip http on page 116**
- **ip http access-class on page 117**
- **ip http max-connection-time on page 118**
- **ip http port on page 119**
- **ip http redirectUrl on page 120**
- **ip http same-host-limit on page 121**
- **ip http server on page 122**
- **ipv6 http on page 123**

- ipv6 http port on page 124
- ipv6 http redirectUrl on page 125
- ipv6 http server on page 126

Using CoA Messages with Guided Entrance Services

Typically, a guided entrance service directs a subscriber to a Web site, where the subscriber can select from a group of available services. When the subscriber selects a new service to use, Service Manager uses a RADIUS CoA message to activate the new service—you can also configure RADIUS to deactivate the original guided entrance service. To inform Service Manager to deactivate the original guided entry service, you must include the Deactivate-Service attribute in the RADIUS records of the services that can be selected from the Web site.

If you configure a guided entrance service, you must also ensure that the router's RADIUS dynamic-request server is enabled and supports CoA messages. See the *Configuring RADIUS Dynamic-Request Server* chapter in this guide, for information about the RADIUS dynamic-request server and CoA messages.

Table 15 on page 91 describes a partial RADIUS Access-Accept message for a guided entrance service and the CoA-Request message for the tiered service that the subscriber subsequently selects from the Web site. The CoA message for the tiered service includes the Deactivate-Service attribute that deactivates the guided entrance service.

Table 15: Deactivating a Guided Entrance Service

Guided Entrance Service Activated at Login		
RADIUS Attribute	Tag	Value
username	none	client5@isp1.com
activate-service	1	http(192.168.25.2, 80)

Tiered Service Selected at Web Site

RADIUS Attribute	Tag	Value
username	none	client5@isp1.com
activate-service	2	tiered(1280000, 5120000)
deactivate-service		http(192.168.25.2, 80)
service-timeout	2	720

RADIUS Attribute	Tag	Value
service-statistics	2	2

Related Documentation

- Guided Entrance Service Overview on page 31
- Redirection of Subscriber Sessions When HTTP Local Server is Disabled or Not Configured on page 32
- Configuring the HTTP Local Server to Support Guided Entrance on page 87
- Example: Guided Entrance Service Definition on page 101

Configuring the Preservation of the Original URL During Redirection of Subscriber Sessions

You can configure the HTTP local server to preserve the URL, originally requested by a user, as a variable in the redirect URL.

- From Profile Configuration mode, enable preservation of the original URL on the HTTP local server.
  - To configure preservation of the original URL on the IPv4 profile:

    ```
    host1(config-profile)#ip http redirectUrl
      “http://ispite.redirect.com/accessDenied.do?url=%(url)” preserveOriginalUrl
    ```

  - To configure preservation of the original URL on the IPv6 profile:

    ```
    host1(config-profile)#ipv6 http redirectUrl
      “http://ispite.redirect.com/accessDenied.do?url=%(url)” preserveOriginalUrl
    ```

NOTE: You must press Ctrl+v before typing “?” in the CLI. You must also ensure that the redirect URL is of the HTTP query type according to the server language supported by the redirect server.

Related Documentation

- Preservation of the Original URL During Redirection of Subscriber Sessions on page 33
- ip http redirectUrl on page 120
- ipv6 http redirectUrl on page 125

Setting a Baseline for HTTP Local Server Statistics

You can set a baseline for HTTP server statistics.

The system implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.

To set a baseline:

- Include the **baseline ip http** command at the User Exec or Privilege Exec level:

  host1#baseline ip http

There is no **no** version.

Related Documentation

- Monitoring Statistics for Connections to the HTTP Local Server on page 140
- baseline ip http

CHAPTER 20

Examples

Example: Combined IPv4 and IPv6 Service in a Dual Stack Service Definition

The following example explains how to create a combined IPv4 and IPv6 service in a dual stack.

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

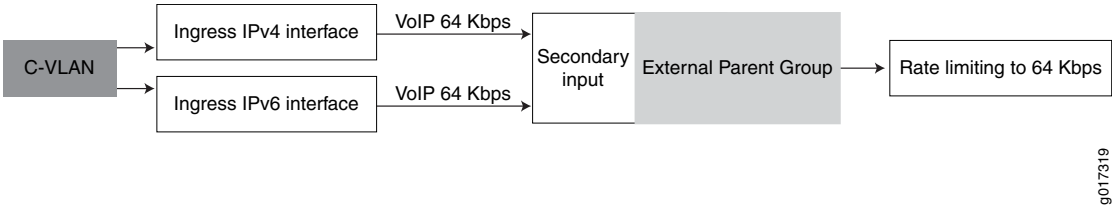
Overview

When you configure a combined IPv4 and IPv6 service in a dual stack, the policies defined in the interface profile are attached to the appropriate interfaces based on the type of the interface. For example, all IPv4 policies are attached to the IPv4 interface and all IPv6 policies are attached to the IPv6 interface.

Figure 5 on page 96 shows a topology in which the C-VLAN interface on the customer edge device is connected to the ingress IPv4 and IPv6 interfaces on the provider edge or E Series router. A combined IPv4/IPv6 service, which contains a hierarchical policy and an external parent group with a rate-limit profile that is associated with the hierarchical

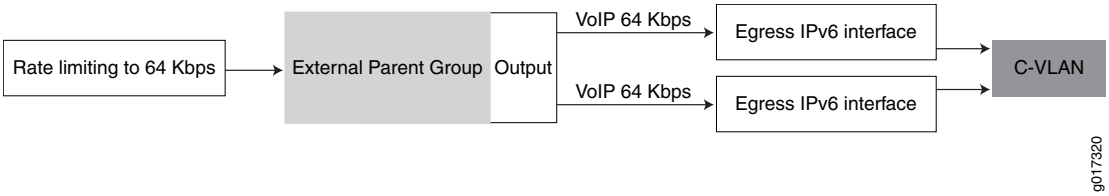
policy, is applied at the secondary input stage on the router. The incoming voice-over-IP classified traffic flows for IPv4 and IPv6 subscribers are allocated a total of 64 Kbps. The common rate limit cannot drop voice-over-IP packets, but must limit the total flow (for IPv4 and IPv6 interfaces) to 64 Kbps.

Figure 5: Input Traffic Flow with Rate-Limit Profile on an External Parent Group for a Combined IPv4/IPv6 Service



Similarly, for traffic flowing from the provider edge device to the C-VLAN interface for voice-over-IP packets, Figure 6 on page 96 shows how the rate-limit profile in the external parent group associated with a hierarchical policy parameter applied to the egress IPv4 and IPv6 interfaces limits the voice-over-IP traffic flowing to the C-VLAN interface on the customer edge device.

Figure 6: Output Traffic Flow with Rate-Limit Profile on an External Parent Group for a Combined IPv4/IPv6 Service



Creating a Combined IPv4 and IPv6 Service

Step-by-Step Procedure

The following example shows the service macro definition file that creates a voice-over-IP service for the topology described above.

```
<# combined_service(inBw, outBw, VBG1, VB6G1, NODE) #>

<# uid := app.servicemanager.getUniqueId #>
<# genericName := "combined-service-" $ uid #>
<# SAClaclName := genericName $ "SA" #>
<# profileName := genericName #>


policy-parameter v4v6-<# uid #> hierarchical
 aggregation-node <# NODE #><# '\n' #>

rate-limit-profile rlpv4v6-<# genericName #>-vb-out one-rate hier
committed-rate <# outBw #><# '\n' #>
committed-action transmit unconditional
conformed-action transmit unconditional

rate-limit-profile rlpv4v6-<# genericName #>-vb-in one-rate hier
committed-rate <# inBw #><# '\n' #>
committed-action transmit unconditional
conformed-action transmit unconditional


parent-group vb-v4v6-<# uid #>-in
 rate-limit-profile rlpv4v6-<# genericName #>-vb-in

parent-group vb-v4v6-<# uid #>-out
 rate-limit-profile rlpv4v6-<# genericName #>-vb-out


classifier-list cl46-4-<# genericName #>-vb-in ip any host <# VBG1 #> <# '\n' #>
classifier-list cl46-4-<# genericName #>-vb-out ip host <# VBG1 #> any

ipv6 classifier-list cl46-6-<# genericName #>-vb-in destination-host <# VB6G1 #><# '\n' #>
ipv6 classifier-list cl46-6-<# genericName #>-vb-out source-host <# VB6G1 #><# '\n' #>


ip policy-list pl-v4v6-<# genericName #>-in
 classifier-group cl46-4-<# genericName #>-vb-in external parent-group vb-v4v6-<# uid #>-in parameter
v4v6-<# uid #><# '\n' #>
  forward


ip policy-list pl-v4v6-<# genericName #>-out
 classifier-group cl46-4-<# genericName #>-vb-out  external parent-group vb-v4v6-<# uid #>-out parameter
 v4v6-<# uid #><# '\n' #>
  forward


ipv6 policy-list pl6-v4v6-<# genericName #>-in
 classifier-group cl46-6-<# genericName #>-vb-in external parent-group vb-v4v6-<# uid #>-in parameter
v4v6-<# uid #><# '\n' #>
  forward

ipv6 policy-list pl6-v4v6-<# genericName #>-out
 classifier-group cl46-6-<# genericName #>-vb-out external parent-group vb-v4v6-<# uid #>-out parameter
v4v6-<# uid #><# '\n' #>
  forward
```

```
profile <# profileName #><# '\n' #>
 ip policy output pl-v4v6-<# genericName #>-out statistics enabled merge
 ip policy secondary-input pl-v4v6-<# genericName #>-in statistics enabled merge
 ipv6 policy output pl6-v4v6-<# genericName #>-out statistics enabled merge
 ipv6 policy secondary-input pl6-v4v6-<# genericName #>-in statistics enabled merge

<# env.setResult("activate-profile", profileName) #>
<# env.setResult("service-interface-type", "ipv4-ipv6") #>
<# env.setResult("secondary-input-stat-epg", "vb-v4v6-"$ uid $"-in v4v6-"$ uid $"") #>
<# env.setResult("output-stat-epg", "vb-v4v6-"$ uid $"-out v4v6-"$ uid $"") #>
<# endtmpl #>
```

In the service definition macro, a hierarchical policy parameter for the rate limit is created with an aggregation node value. The aggregation node stores a single rate-limit instance and statistics for this rate-limit. An external rate-limit aggregation node can be defined by the 4-tuple (slot, direction, external parent group name, parameter value). Each reference to a policy parameter in a policy is substituted with its value for all attachments of this policy at the interface.

Two rate-limit profiles are created, one each for the ingress and egress interfaces. Rate limiters are implemented using a dual token bucket scheme: a token bucket for conformed (yellow) packets and a token bucket for committed (green) packets. The following are the attributes configured in the rate-limit profile applied to ingress and egress interfaces:

- The committed rate for the rate-limit profile is entered as a specified value.
- The committed action, which specifies the action for packets conforming to the committed rate and committed burst size and conforming to the exceed rate and exceed burst size for a rate-limit profile is set to receive transmit unconditional.
- The conformed action, which sets the action for packets not conforming to the committed rate and committed burst size, but conforming to the peak rate and peak burst size for a rate-limit profile is set to receive transmit unconditional.

Two external parent groups, one each for the ingress and egress interfaces, that reference the rate-limit profiles created for incoming and outgoing traffic, are created and specified in the service definition.

Classifier control lists for ingress IPv4 and IPv6 traffic, and for egress IPv4 and IPv6 traffic, are also created. These classifiers classify traffic based on source and destination addresses.

The input and output classifier lists for IPv4 traffic are used in IP policy lists that are attached to the ingress and egress IPv4 interfaces respectively. The input and output classifier lists for IPv6 traffic are used in IPv6 policy lists that are attached to the ingress and egress IPv6 interfaces respectively. The **external parent-group** keyword creates an external parent group in a rate-limit hierarchy for IPv4 and IPv6. All packets matching the classifier are sent to the parent group for further processing.

The policy lists for voice-over-IP traffic are configured in the service definition macro file that creates a combined IPv4/IPv6 service to be applied to the ingress IPv4 and IPv6 interfaces.

A profile is created that you want to attach to the service session. The IPv4 and IPv6 policies for voice-over-IP traffic arriving at the IPv4 and IPv6 interfaces respectively are applied to the secondary input stage. The IPv4 and IPv6 policies for voice-over-IP traffic leaving the IPv4 and IPv6 interfaces respectively are applied to the output stage. Statistics collection is enabled for the policies referenced in the service macro using the **statistics enabled** keyword in the command used for policy attachment in the profile. The **merge** keyword enables merging of multiple policies to form a single policy.

The **<# env.setResult("activate-profile", profileName) #>** command specifies the interface profile to be used on activation of the interface. After the subscriber service session is activated, the policies defined in the interface profile are applied to both IPv4 and IPv6 interfaces. The elements in the profile to be attached to the interfaces are determined by the type of the interface.

The **<# env.setResult("service-interface-type", "ipv4-ipv6") #>** command configures the service macro to be used for IPv4 and IPv6 interfaces in a dual stack. The profile identifier returned from the activate-profile object will be applied to both IPv4 and IPv6 interfaces.

The service definition macro is configured to collect input and output statistics associated with external parent groups in a hierarchical policy for IPv4 and IPv6 subscribers as follows:

```
<# env.setResult("secondary-input-stat-epg", "vb-v4v6-"$ uid $"-in v4v6-"$ uid $"") #>
<# env.setResult("output-stat-epg", "vb-v4v6-"$ uid $"-out v4v6-"$ uid $"") #>
```

The <# env.setResult("secondary-input-stat-epg", "vb-v4v6-"$ uid $"-in v4v6-"$ uid $"") #> command specifies that Service Manager track statistics associated with the external parent group named vb-v4v6-in and the corresponding hierarchical policy named v4v6, and that this external parent group is associated with the policy that is attached at the input stage.

The **<# env.setResult("output-stat-epg", "vb-v4v6-"$ uid $"-out v4v6-"$ uid $"") #>** command specifies that Service Manager track the output statistics associated with the external parent group named vb-v4v6-out and the corresponding hierarchical policy named v4v6, which is associated with the policy attached at the output stage.

The input and output statistics associated with the external parent group are collected and forwarded to the Service Manager to be displayed in the Acct-Stop and Interim-Acct messages.

If you use the **secondary-input-stat-clacl** and **output-stat-clacl** objects in the service macro to track Service Manager statistics, the values returned in the output of the **show service-management** command do not accurately reflect the packets that are rate-limited. In this case, although some of the packets that were classified by the classifier lists are dropped by the rate-limiter on the external parent group, the Service Manager statistics collection application counts all the packets that were classified without excluding those that were dropped by the rate limiter. As a result, the values returned by the **output-stat-clacl** and **secondary-input-stat-clacl** objects represent more packets than those sent to the subscriber and core interfaces respectively.

Using the macro that has been described here, you can configure the following combined service, for example:

combined_service(64000, 64000, 10.0.0.1, 2001::1, vlan)

where

- 64000—Bandwidth for outbound traffic, denoted as *outBw* in the macro
- 64000—Bandwidth for inbound traffic, denoted as *inBw* in the macro
- 10.0.0.1—Host IP address for IPv4 subscribers, denoted as *VBG1* in the macro
- 2001::1—Host IP address for IPv6 subscribers, denoted as *VB6G1* in the macro
- vlan—Interface on which the service is configured, denoted as *NODE* in the macro

Related Documentation

- Combined and Independent IPv4 and IPv6 Services in a Dual Stack Overview on page 21
- Activation and Deactivation of IPv4 and IPv6 Services in a Dual Stack on page 61
- Service Interim Accounting for IPv4 and IPv6 Services in a Dual Stack Overview on page 27
- Configuring the HTTP Local Server to Support Guided Entrance on page 87

Example: Guided Entrance Service Definition

The following example shows you how to create a guided entrance service.

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Overview

When a subscriber logs in and opens a Web browser, the Service Manager guided entrance service transparently directs the subscriber to a specific uniform resource locator (URL) at which the subscriber can choose from a list of available services.

Creating a Guided Entrance Service

Step-by-Step Procedure This example illustrates how to create a guided entrance service:

NOTE: Commented text explains the parameterized values in the example of the service definition macro file. Each example is followed by examples of RADIUS information and the CLI command that you can use to activate a subscriber service session.

```
!parameterizes server address and port
<# http(serverIp, serverPort) #>

<# serviceTag := "http-" #>
<# uid := app.servicemanager.getUniqueId #>
<# genericName := "SM-X-" $ serviceTag $ uid #>
<# genericInputName := "SM-I-" $ serviceTag $ uid #>
<# genericOutputName := "SM-O-" $ serviceTag $ uid #>
<# claclName := genericName #>

<# profileName := genericName #>
<# inputPolicyName := genericInputName #>
<# inputRateLimitName := genericInputName #>
<# outputPolicyName := genericOutputName #>
<# outputRateLimitName := genericOutputName #>

<# exceptionClaclName := "exceptionClaclPort" $ serverPort #>
<# serverClaclName := "serverClaclIp" $ serverIp #>
<# redirectUrlName := "http://" $ serverIp $ ":" $ serverPort #>

configure terminal

classifier-list <# serverClaclName #> ip any host <# serverIp; '\n' #>

classifier-list <# exceptionClaclName #> tcp any any eq <# serverPort; '\n' #>

ip policy-list <# inputPolicyName; '\n' #>
classifier-group <# serverClaclName; '\n' #>
        forward
    classifier-group <# exceptionClaclName; '\n' #>
        exception http-redirect
    classifier-group *
        filter

profile <# profileName #>
    ip http redirectUrl <# redirectUrlName; '\n' #>
    ip policy input <# inputPolicyName #> statistics enabled merge

<# env.setResult("activate-profile", "" $ profileName) #>

<# endtmpl #>
```

Sample RADIUS Attributes

Step-by-Step Procedure

Table 16 on page 104 provides the sample RADIUS attributes that you can use to activate the guided entrance service

Table 16: Sample RADIUS Attributes

RADIUS Attribute	Tag	Value
username	none	client5@isp1.com
activate-service	1	http(192.168.25.2, 80)

Sample CLI Command

Step-by-Step Procedure

To activate a subscriber session with the configured guided entrance service:

```
host1(config)#service-management subscriber-session client5@isp1.com interface atm
5/0.1 service-session " http(192.168.25.2, 80)"
```

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- Guided Entrance Service Overview on page 31
- Configuring the HTTP Local Server to Support Guided Entrance on page 87
- Using CoA Messages with Guided Entrance Services on page 91
- **service-management subscriber-session service-session on page 132**

Example: Tiered Service Definition

The following example shows you how to create a tiered service.

- Requirements on page 104
- Overview on page 105
- Creating a Tiered Service on page 105

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)

- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Also, this example assumes that QoS profile triplePlayIP and QoS parameter maxSubscBW are configured.

Overview

A tiered service typically provides set bandwidths for both inbound and outbound traffic for a subscriber. In this example, the bandwidth values are parameterized.

Creating a Tiered Service

Step-by-Step Procedure This example illustrates how to create a tiered service:

NOTE: Commented text explains the parameterized values in the example of the service definition macro file. Each example is followed by examples of RADIUS information and the CLI command that you can use to activate a subscriber service session.

```
!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>
classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
  committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
  classifier-group matchAll precedence 10000
   rate-limit-profile <# name; '\n' #>
   traffic-class best-effort

policy-list <# oname; '\n' #>
  classifier-group matchAll precedence 10000
   traffic-class best-effort

profile <# name; '\n' #>
  ip policy secondary-input <# name #> statistics enabled merge
  ip policy output <# oname #> statistics enabled merge
  qos-profile triplePlayIP
  qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clacl", "matchAll") #>
<# env.setResult("output-stat-clacl", "matchAll") #>

<# endtmpl #>
```

Sample RADIUS Attributes

Step-by-Step Procedure

Table 17 on page 106 provides the sample RADIUS attributes that you can use to activate the tiered service

Table 17: Sample RADIUS Attributes

RADIUS Attribute	Tag	Value
username	none	client1@isp1.com
activate-service	1	tiered(1280000, 5120000)

Sample CLI Command

Step-by-Step Procedure

To activate a subscriber session with the configured tiered service:

```
host1(config)#service-management subscriber-session client1@isp1.com  interface atm
  4/0.1 service-session "tiered(1280000, 5120000)"
```

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- **service-management subscriber-session service-session on page 132**

Example: Video-on-Demand Service Definition

The following example shows a sample service definition macro file that creates a video-on-demand service—the service provides bandwidth that meets the needs of video streams.

- Requirements on page 106
- Overview on page 107
- Creating a Video-on-Demand Service on page 107

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Overview

The video-on-demand service definition creates the bandwidth towards the subscriber and parameterizes the source of the video feed.

Creating a Video-on-Demand Service

Step-by-Step Procedure This example illustrates how to create a video-on-demand service:

NOTE: Commented text explains the parameterized values in the example of the service definition macro file. Each example is followed by examples of RADIUS information and the CLI command that you can use to activate a subscriber service session.

```
!parameterizes download bandwidth and server address
<# videoMin(downloadBW, serverAddress) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-video-" $ uid #>

classifier-list <# name #> ip any <# serverAddress #> 0.0.0.0

policy-list <# name; '\n' #>
   classifier-group <# name #> precedence 5000
    traffic-class video

profile <# name; '\n' #>
   ip policy output <# name #> statistics enabled merge
   qos-parameter maxVideoBW add <# downloadBW; '\n' #>
   exit

<# env.setResult("activate-profile", name) #>
<# env.setResult("output-stat-clacl", name) #>

<# endtmpl #>
```

Sample Owner ID

Step-by-Step Procedure Table 18 on page 107 provides the sample RADIUS attributes that you can use to activate the video-on-demand service

Table 18: Sample RADIUS Attributes

Owner	Owner ID	Value
AAA (RADIUS)	Acct-Session-ID (RADIUS attribute 44)	573498

Sample CLI Command

Step-by-Step Procedure

To activate a subscriber session with the configured video-on-demand service:

```
host1(config)#service-management owner-session aaa 573498 service-session "
  videoMin(4500000, 192.168.23.58)"
```

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- **service-management subscriber-session service-session on page 132**

Example: Voice-over-IP Service Definition

The following example shows you how to create a voice-over-IP (VoIP) service.

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Overview

A VoIP service is a session border controller (SBC) media gateway (MG)-based service that has upstream and downstream components.

The IP address and port for both the subscriber and the opposite end of the phone call were originally negotiated with the SBC. The VoIP service learns the IP addresses and ports for both ends of the call, and then specifies that any traffic to either end is put in the voice traffic class.

Creating a Voice-over-IP Service

Step-by-Step Procedure This example illustrates how to create a VoIP service:

NOTE: Commented text explains the parameterized values in the example of the service definition macro file. Each example is followed by examples of RADIUS information and the CLI command that you can use to activate a subscriber service session.

```
!parameterizes source address and port, destination address and port, and protocol type
<# mgFlow(upDA, upDPort, downDA, downDPort, protType) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-mgFlow-" $ uid #>
<# oname := "SM-O-mgFlow-" $ uid #>

classifier-list <# name #> <# protType #> any <#upDA #> 0.0.0.0 eq <# upDPort; '\n' #>
policy-list <# name; '\n' #>
   classifier-group <# name #> precedence 2000
    traffic-class voice
    forward

classifier-list <# oname #> <# protType #> any <#downDA #> 0.0.0.0 eq <# downDPort; '\n' #>
policy-list <# oname; '\n' #>
   classifier-group <# oname #> precedence 2000
    traffic-class voice
    forward

profile <# name ; '\n' #>
   ip policy input <# name #> statistics enabled merge
   ip policy output <# oname #> statistics enabled merge

<# env.setResult("activate-profile", name) #>

<# endtmpl #>
```

Sample RADIUS Attributes

Step-by-Step Procedure Table 19 on page 109 provides the sample RADIUS attributes that you can use to activate the VoIP service

Table 19: Sample RADIUS Attributes

RADIUS Attribute	Tag	Value
username	none	client1@isp1.com
activate-service	1	mgFlow(10.10.10.10, 1234, 192.168.45.54, 1234, udp)

Sample CLI Command

Step-by-Step Procedure

To activate a subscriber session with the configured VoIP service:

```
host1(config)#service-management subscriber-session client1@isp1.com  interface atm
4/0.1 service-session “mgFlow(10.10.10.10, 1234,  192.168.45.54, 1234, udp)”
```

Related Documentation

- Service Definitions Overview on page 9
- Creating Service Definitions on page 41
- Managing Your Service Definitions on page 44
- Understanding Service Manager RADIUS Attributes on page 15
- Understanding RADIUS Accounting for Service Manager on page 23
- **service-management subscriber-session service-session on page 132**

CHAPTER 21

Configuration Commands

aaa service accounting interval

Syntax aaa service accounting interval *period*

no aaa service accounting interval

Release Information Command introduced in JunosE Release 9.0.0.

Description Specifies the default accounting interval used for services on the virtual router—the Service Manager application uses this setting for RADIUS-initiated services when no value is specified in the Service-Interim-Acct-Interval VSA (Juniper VSA 26-140). The **no** version restores the default setting of 0, which turns off interim accounting for services associated with users attached to this virtual router.

NOTE: This command and the **aaa user accounting interval** command replace the deprecated **aaa accounting interval** command, which may be removed completely in a future release.

Options

- *period*—Accounting interval in minutes in the range 10–1440, which sets the time period between accounting updates for services associated with users on this virtual router; 0 is the default

Mode Global Configuration

aaa user accounting interval

Syntax aaa user accounting interval *period*

no aaa user accounting interval

Release Information Command introduced in JunosE Release 9.0.0.

Description Specifies the default user accounting interval used on the virtual router. This router uses this value for users when no value is specified in the RADIUS Acct-Interim-Interval attribute (RADIUS attribute 85). The **no** version restores the default setting of 0, which turns off interim accounting for users attached to this virtual router.

NOTE: **This command and the aaa service accounting interval command replace the deprecated aaa accounting interval command, which may be removed completely in a future release.**

Options

- *period*—Accounting interval in minutes in the range 10–1440, which sets the time period between accounting updates for users on this virtual router; 0 is the default

Mode Global Configuration

copy

Syntax copy [sourcePath]*sourceFilename* [*destinationPath*]*destinationFilename* [force]

Release Information Command introduced before JunosE Release 7.1.0.
hostName and *deviceName* variables added in JunosE Release 7.2.0.

Description Copies a local or network file. There is no **no** version.

NOTE:

- You cannot change the extension of a file, for example, from .mac to .scr. You can copy software release (.rel) files only *to* the router (download); you cannot copy them *from* the router (upload). See *Copying and Redirecting Files* in the *JunosE System Basics Configuration Guide*, for detailed information on file type usage with the **copy** command.
- You cannot copy script (.scr) or macro (.mac) files while in Boot mode. You can copy only .cnf, .hty, and .rel files. If you issue the **dir** command from Boot mode, existing .scr and .mac files are not displayed.

Options

- sourcePath—Path to the source in the format:
  hostName: | *deviceName*: | /incoming*/subdirectory/* | /outgoing*/subdirectory/*
- *hostName*:—Name of the network host
- *deviceName*:—Name of the device specifying a flash card slot
  - disk0—Specifies flash card slot 0 on the primary SRP module; if no device is specified for the primary SRP module, then disk0 is used
  - disk1—Specifies flash card slot 1 on the primary SRP module; source and destination file types must be .dmp; supported only on the E120 and E320 routers
  - standby—Specifies flash card slot 0 on the standby SRP module for backward compatibility
  - standby-disk0—Specifies flash card slot 0 on the standby SRP module
  - standby-disk1—Specifies flash card slot 1 on the standby SRP module; source and destination file types must be .dmp; supported only on the E120 and E320 routers
  - incoming—Specifies the router's incoming FTP directory
  - *subdirectory*—Name of a subdirectory on the router's FTP server. If the subdirectory does not exist, the router creates it.
  - outgoing—Specifies the router's outgoing FTP directory
- *sourceFilename*—Name of the source file
- destinationPath—Path to the destination in the format:
  networkPath | /incoming*/subdirectory* | /outgoing*/subdirectory*

- *networkPath*—Path to the network host
- incoming—Specifies the incoming router's FTP directory
- *subdirectory*—Name of a subdirectory on the *ERX* router's FTP server. If the subdirectory does not exist, the router creates it.
- outgoing—Specifies the router's outgoing FTP directory

- *destinationFilename*—Name of the destination file
- force—Forces a copy, even when the destination file already exists; if a file is marked by the file system as in use because it is required for the current operation or configuration, the **force** keyword cannot force a copy of that file

Mode Privileged Exec

ip http

Syntax [no] ip http

Release Information Command introduced in JunosE Release 7.2.0.

Description Creates the HTTP local server. The **no** version deletes the HTTP local server.

Mode Global Configuration

ip http access-class

Syntax ip http access-class *listName*

no ip http access-class

Release Information Command introduced in JunosE Release 7.2.0.

Description Specifies the standard IP access list that identifies the subscribers who are authorized to connect to the HTTP local server. The **no** version removes the association between the access list and the HTTP local server.

Options
- *listName*—Name of the access list

Mode Global Configuration

ip http max-connection-time

Syntax ip http max-connection-time *seconds*

no ip http max-connection-time

Release Information Command introduced in JunosE Release 7.2.0.

Description Specifies the maximum time that the HTTP local server maintains an inactive connection. The **no** version restores the default time.

Options
- *seconds*—Either 0 (unlimited) or the number of seconds in the range 3–7200; default value is 30 seconds

Mode Global Configuration

ip http port

Syntax ip http port *portNumber*

no ip http port

Release Information Command introduced in JunosE Release 7.2.0.

Description Specifies the port on which the HTTP local server receives connection attempts. The **no** version restores the default port number.

Options
- *portNumber*—Number of the port, in the range 0–65535; the default is port 80

Mode Global Configuration

ip http redirectUrl

Syntax

ip http redirectUrl *url* [preserveOriginalUrl]

no ip http redirectUrl

Release Information

Command introduced in JunosE Release 7.2.0.
preserveOriginalUrl keyword added in JunosE Release 12.3.0.

Description

Specifies the URL to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber. The **no** version removes the redirection action.

Options

- *url*—Name of the URL; 230 characters maximum
- preserveOriginalUrl —Enables the preservation of the subscriber's originally requested URL

Mode

Interface Configuration, Profile Configuration, Subinterface Configuration

Related Documentation

- Configuring the Preservation of the Original URL During Redirection of Subscriber Sessions on page 92

ip http same-host-limit

Syntax ip http same-host-limit *maxConnections*

no ip http same-host-limit

Release Information Command introduced in JunosE Release 7.2.0.

Description Specifies the maximum number of connections that can exist between one IP address and the HTTP local server. The **no** version restores the default number of allowed connections.

Options
- *maxConnections*—Maximum number of connections allowed, in the range 0–1000; the default is 3

Mode Global Configuration

ip http server

Syntax [no] ip http server

Release Information Command introduced in JunosE Release 7.2.0.

Description Enables the HTTP local server. The **no** version disables the HTTP local server.

Mode Global Configuration

ipv6 http

Syntax [no] ipv6 http

Release Information Command introduced in JunosE Release 10.1.0.

Description Creates the HTTP local server for IPv6. The **no** version deletes the HTTP local server.

Mode Global Configuration

Related Documentation
- *Configuring the HTTP Server to Support Guided Entrance* in the *JunosE Broadband Access Configuration Guide*

ipv6 http port

Syntax ipv6 http port *portNumber*

no ipv6 http port

Release Information Command introduced in JunosE Release 10.1.0.

Description Specifies the port on which the HTTP local server receives connection attempts for IPv6. The **no** version restores the default port number.

NOTE: Port numbers from 1 to 1024 are known as reserved ports. We recommend that you specify a port number that does not belong to this range.

Options

- *portNumber*—Number of the port, in the range 0–65535; the default is port 80

Mode Global Configuration

Related Documentation

- *Configuring the HTTP Server to Support Guided Entrance* in the *JunosE Broadband Access Configuration Guide*

ipv6 http redirectUrl

Syntax ipv6 http redirectUrl *url* [preserveOriginalUrl]

no ipv6 http redirectUrl

Release Information Command introduced in JunosE Release 10.1.0.
Profile Configuration mode added in JunosE Release 11.0.0.
preserveOriginalUrl keyword added in JunosE Release 12.3.0.

Description Specifies the URL to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber. The first access session is typically used by the Service Manager application to provide initial provisioning and service selection for the subscriber. The **no** version removes the redirection action.

NOTE: **The HTTP local server must be configured and enabled in the virtual router for the interface on which you use this command. Otherwise, the URL redirect operation will fail.**

Options

- *url*—Name of the URL; 230 characters maximum
- preserveOriginalUrl —Enables the preservation of the subscriber's originally requested URL

Mode Interface Configuration, Subinterface Configuration, Profile Configuration

Related Documentation

- Configuring the Preservation of the Original URL During Redirection of Subscriber Sessions on page 92

ipv6 http server

Syntax [no] ipv6 http server

Release Information Command introduced in JunosE Release 10.1.0.

Description Enables the HTTP local server to listen for and process IPv6 exception packets. The **no** version disables the HTTP local server.

Mode Global Configuration

Related Documentation
- *Configuring the HTTP Server to Support Guided Entrance* in the *JunosE Broadband Access Configuration Guide*

profile

Syntax To assign a profile name for a remote host:

[no] profile *profileName*

To create a profile or assign a profile to an interface:

profile [bridgedEthernet | ip | l2tp | ppp | pppoe | vlan | any] *profileName*

no profile [bridgedEthernet | ip | l2tp | ppp | pppoe | vlan | any]

Release Information Command introduced before JunosE Release 7.1.0.
vlan keyword added in JunosE Release 7.1.0.
IP Tunnel Destination Profile Configuration mode added in JunosE Release 8.2.0.

Description When used from Global Configuration mode, creates a profile. Use profiles to configure interfaces dynamically, which enables you to manage a large number of interfaces effectively. The **no** version removes the profile.

When used from Interface Configuration mode and Subinterface Configuration mode, assigns a profile to an interface. Use profiles to configure interfaces dynamically, which enables you to manage a large number of interfaces effectively. The **no** version removes the profile assigned to the interface.

When used in IP Tunnel Destination Profile Configuration mode, defines an IP profile with parameters that are used to stack an upper IP interface over a dynamic GRE or DVMRP tunnel. The **no** version removes the IP profile from the destination profile.

When used from L2TP Destination Profile Host Configuration mode, sets an attribute of the current remote host. The **no** version removes the attribute from the remote host.

Options

- bridgedEthernet—Specifies a bridged Ethernet encapsulation type to which the profile applies
- ip—Specifies an IP encapsulation type to which the profile applies
- l2tp—Specifies an L2TP encapsulation type to which the profile applies
- ppp—Specifies a PPP encapsulation type to which the profile applies
- pppoe—Specifies a PPPoE encapsulation type to which the profile applies
- vlan—Specifies a VLAN encapsulation type to which the profile applies
- any—Specifies any autoconfigured encapsulation that does not have a specific profile assignment
- *profileName*—Profile name of up to 80 characters

Mode Global Configuration, Interface Configuration, IP Tunnel Destination Profile Configuration, L2TP Destination Profile Host Configuration, Subinterface Configuration

qos-profile

Syntax [no] qos-profile *qosProfileName*

Release Information Command introduced before JunosE Release 7.1.0.
Profile Configuration mode added in JunosE Release 7.2.0.
QoS Interface Set Configuration and QoS Interface Superset Configuration modes added in JunosE Release 9.2.0.

Description In Global Configuration mode, creates a QoS profile on the router and enters QoS Profile Configuration mode. The **no** version deletes the QoS profile.

In Interface Configuration mode, attaches a QoS profile to an interface. The **no** version detaches the QoS profile from the interface.

In Profile Configuration mode, adds a QoS profile command for use with Service Manager. When the service is activated, the QoS profile is created and attached to the subscriber interface. The **no** version removes the QoS profile from the profile.

In QoS Interface Set Configuration mode, attaches a QoS profile to the QoS interface set. The **no** version detaches the QoS profile from the interface set.

In QoS Interface Superset Configuration mode, attaches a QoS profile to the QoS interface superset. The **no** version detaches the QoS profile from the interface superset.

Options
- *qosProfileName*—Name of the QoS profile

Mode Global Configuration, Interface Configuration, Profile Configuration, QoS Interface Set Configuration, QoS Interface Superset Configuration

Related Documentation
- Configuring a QoS Profile
- Attaching a QoS Profile to an Interface
- Configuring Shadow Nodes
- Configuring a Basic Parameter Definition for QoS Administrators
- Creating Parameter Instances
- Attaching a QoS Profile to an Interface Superset or an Interface Set
- Creating a QoS Parameter on an Interface Superset or Interface Set

service-management install

Syntax [no] service-management install *fileName*.mac

Release Information Command introduced in JunosE Release 7.2.0.

Description Installs the specified Service Manager definition. The **no** version removes the specified definition.

Options
- *fileName*—Name of the service definition macro file, including the .mac extension

Mode Global Configuration

service-management service-session-profile

Syntax [no] service-management service-session-profile *profileName*

Release Information Command introduced in JunosE Release 7.2.0.

Description Creates a new Service Manager service session profile or specifies the name of an existing service session profile, then enters Service Session Profile Configuration mode. The **no** version removes the service session profile.

Options
- *profileName*—Name of the service session profile

Mode Global Configuration

service-management owner-session

Syntax [no] service-management owner-session *ownerName ownerId* service-session *serviceName* [service-session-profile *profileName*]

Release Information Command introduced in JunosE Release 8.0.0.

Description Activates subscriber service sessions based on the specified owner and owner-generated ID. The **no** version gracefully removes the specified service session for the specified owner session.

Privileged Exec mode creates a dynamic subscriber service session that is deleted after a router reboot. Global Configuration mode creates a persistent service session.

Options

- *ownerName*—Name of the owner for the owner session; AAA for RADIUS-based subscribers
- *ownerId*—Unique ID that is generated by the owner; Acct-Session-ID for AAA subscriber sessions
- *serviceName*—Name of the service session to use
- *profileName*—Name of the service session profile to use for the service session

Mode Global Configuration, Privileged Exec

service-management subscriber-session service-session

Syntax [no] service-management subscriber-session *subscriberName* interface *interfaceType interfaceSpecifier* service-session *serviceName* | [service-session-profile *profileName*]

Release Information Command introduced in JunosE Release 7.2.0.
Privileged Exec mode added in JunosE Release 8.0.0.

Description Activates a subscriber session and service session for the specified subscriber. The **no** version gracefully removes all service sessions or the specified service session.

Privileged Exec mode creates a dynamic subscriber session that is deleted after a router reboot. Global Configuration mode creates a persistent subscriber session.

Options

- *subscriberName*—Name of the subscriber for this subscriber session
- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
- *serviceName*—Name of the service session to use for this subscriber session
- *profileName*—Name of the service session profile to use for this service session

Mode Global Configuration, Privileged Exec

statistics

Syntax statistics { time | volume-time }

no statistics

Release Information Command introduced in JunosE Release 7.2.0.

Description Enables statistics for the service session profile. The **no** version disables statistics for the service session profile.

Options
- time—Displays statistics for the time attribute
- volume-time—Displays statistics for both the volume and time attributes

Mode Service Session Profile Configuration

time

Syntax time *seconds*

no time

Release Information Command introduced in JunosE Release 7.2.0.

Description Configures the threshold for the amount of time that the service session can be active for a subscriber. The service is terminated when the time expires. The **no** version removes the time attribute from the service session profile.

Options
- *seconds*—Number of seconds in the range 0–16777251

Mode Service Session Profile Configuration

volume

Syntax volume *megabytes*

no volume

Release Information Command introduced in JunosE Release 7.2.0.

Description Configures the threshold for the volume of traffic allowed for the service session. The service is terminated when the threshold is exceeded. The **no** version removes the volume attribute from the service session profile.

Options
- *megabytes*—Number of megabytes in the range 0–16777251

Mode Service Session Profile Configuration

PART 3

Administration

CHAPTER 22

Monitoring HTTP Local Server Settings

Monitoring Profiles for the HTTP Local Server

Purpose Display information about the redirect URL used for guided entrance services.

Action To display information about the redirect URL used by the HTTP local server:

```
host1#show profile name guidedProfile2
Profile                    : guidedProfile2
.
.
.
Auto Detect                : Disabled
Auto Configure             : Disabled
IP FlowStats               : Disabled

Ip http redirect Url : myredirect.html

Ipv6 http redirect Url: myredirect.html
```

Meaning Table 20 on page 139 lists the **show profile** command output fields.

Table 20: show profile Output Fields

Field Name	Field Description
Ip http redirect Url	URL of the Web page used for Service Manager guided entrance services for IPv4
Ipv6 http redirect Url	URL of the Web page used for Service Manager guided entrance services for IPv6

Related Documentation

- show profile on page 171

Monitoring Statistics for Connections to the HTTP Local Server

Purpose Display statistics about the connections to the HTTP local server.

Action To display statistics about HTTP local server with the baseline values subtracted:

```
host1#show ip http statistics delta
  Server enable count: 1
  Server disable count: 0
  Same host enforced: 0
  Access class denies: 0
  No resource failures: 0
  Http connections created: 2
  Http connections terminated: 2
  Http connections aged out: 1
  Urls successfully served: 0
  Malformed http requests: 0
  Urls not found: 0
```

Meaning Table 21 on page 140 lists the **show ip http statistics** command output fields.

Table 21: show ip http statistics Output Fields

Field Name	Field Description
Server enable count	Total number of enabled HTTP local servers
Server disable count	Total number of disabled HTTP local servers
Same host enforced	Number of connections dropped because the limit for connections from one IP address to the HTTP local server was exceeded
Access class denies	Number of connections dropped because of a problem with the standard IP access list that defines the hosts that can access the HTTP local server
No resource failures	Number of connections dropped because of system memory limitations
Http connections created	Total number of HTTP connections established
Http connections terminated	Total number of HTTP connections ended
Http connections aged out	Total number of HTTP connections that expired because they exceeded the maximum allowed connection time
Urls successfully served	Total number of Web pages displayed
Malformed http requests	Number of HTTP requests that failed because the format was incorrect
Urls not found	Number of Web pages not found

Related Documentation

- show ip http on page 170 statistics

Monitoring the Configuration of the HTTP Local Server

Purpose Display information about the configuration of the HTTP local server.

Action To display information about the HTTP local server:

```
host1#show ip http server
  Admin status: enabled
  Access class: not defined
  Listening port: 80
  Same host limit: 3
  Protocol: IPv6
```

Meaning Table 22 on page 141 lists the **show ip http server** command output fields.

Table 22: show ip http server Output Fields

Field Name	Field Description
Admin status	Status of the HTTP local server in the software: enabled or disabled. Enabled implies that the HTTP local server can listen for IPv4 , IPv6, or both IPv4 and IPv6 exception packets.
Access class	Name of a standard IP access list that determines which hosts can log on to the HTTP local server
Listening port	Port that the HTTP local server uses to track requests for connection
Same host limit	Maximum number of connections allowed between one IP address and the HTTP local server
Protocol	Protocols that the HTTP local server is listening for: IPv4, IPv6, or IPv4 and IPv6.

Related Documentation

- show ip http on page 170 server

Monitoring the Connections to the HTTP Local Server

Purpose Display information about the connections to the HTTP local server.

Action To display information about the HTTP local server:

```
host1#show ip http scalar
  Maximum connection length: 1000 seconds
  Current number of http servers: 5
  Number of enabled http servers: 2
```

```
Current number of http connections: 15
Peak number of http connections: 125
Maximum number of http connections: 1000
```

Meaning Table 23 on page 142 lists the **show ip http scalar** command output fields.

Table 23: show ip http scalar Output Fields

Field Name	Field Description
Maximum connection length	Maximum time that the HTTP local server maintains an inactive connection, in seconds
Current number of http servers	Number of configured Web servers
Number of enabled http servers	Number of Web servers enabled
Current number of http connections	Number of connections from subscribers to HTTP local servers
Peak number of http connections	Highest number of connections from subscribers to HTTP local servers
Maximum number of http connections	Maximum number of connections allowed from subscribers to HTTP local servers

Related Documentation

- show ip http on page 170 scalar

CHAPTER 23

Monitoring Accounting for Service Manager

Monitoring the Default Interval for Interim Accounting of Services

Purpose Display the default interval used for interim accounting for services associated with users on the virtual router. An entry of 0 indicates that the feature is disabled.

Action To display the default interval used for interim accounting:

```
host1:vrXyz7#show aaa service accounting interval
service-acct-interval 60
```

Meaning Table 24 on page 143 lists the **show aaa service accounting interval** command output fields.

Table 24: show aaa service accounting interval Output Fields

Field Name	Field Description
service-acct-interval	Value of the default interval

Related Documentation

- show aaa service accounting interval on page 172

Verifying Computation of Service Session Accounting Based on Scheduler Profiles

Purpose Display whether the capability to compute accounting details based on scheduler profiles for policies, with rate-limit profiles in hierarchical parent groups, on output interfaces is enabled.

Action To determine whether the mechanism to calculate accounting details for subscriber service sessions based on scheduler profiles for policies, with rate-limit profiles in hierarchical parent groups, on output interfaces is enabled:

```
host1#show service-accounting-statistics
Service accounting mode is scheduler based.
```

Related Documentation

- Configuring Calculation of Service Session Accounting Based on Scheduler Profiles Instead of Rate-Limit Profiles in Hierarchical Parent Groups for Forwarded Packets on page 64
- service-accounting-statistics scheduler-based
- show service-accounting-statistics

CHAPTER 24

Monitoring Service Manager, Definitions, and Profiles

Monitoring the Status of the Service Manager License

Purpose Display the status of the Service Manager license.

Action To display the status of the Service Manager license:

```
host1#show license service-management
service management license is set
```

Meaning Table 25 on page 145 lists the **show license service-management** command output fields.

Table 25: show license service-management Output Fields

Field Name	Field Description
service management license	Status of the license: set (enabled) or not set (disabled)

Related Documentation

- show license on page 173 service-management

Monitoring IPv4 and IPv6 Interfaces for Service Manager

Purpose Display status information about the IP and IPv6 interfaces.

Action To display information about a specific IP interface.

```
host1#show ip interface gigabitEthernet 1/1.200
GigabitEthernet1/1 line protocol Ethernet is up, ip is not present
  Network Protocols: IP
```

```
  Multipath mode = hashed
  Auto Configure = disabled
  Auto Detect = disabled
  Inactivity Timer = disabled
  Use Framed Routes = disabled
  ARP spoof checking = disabled
  Warm-restart initial-sequence-preference: Operational = 0 Administrative = 0

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0

  queue 0: traffic class best-effort, bound to ip GigabitEthernet1/1
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

Http Redirect Url: http://www.juniper.net
```

To display information about a specific IPv6 interface.

```
host1#show ipv6 interface FastEthernet 9/0.6
FastEthernet9/0.6 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop6
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31cd
  Internet address: 6:1:1::1/64
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 8, Bytes 768
    Unicast Packets 8, Bytes 768
```

```
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 5, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 5

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

IPv6 policy input ipv6InPol25
    rate-limit-profile Rlp2Mb classifier-group clgA entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp8Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy output ipv6PolOut2
    rate-limit-profile RlpOutA classifier-group clgB entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile RlpOutB
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy local-input ipv6PolLocIn5
    rate-limit-profile Rlp1Mb classifier-group clgC entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp5Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0
Http Redirect Url: http://www.juniper.net
```

Meaning Table 26 on page 147 lists the **show ip interface** command output fields.

Table 26: show ip interface Output Fields

Field Name	Field Description
interface	Interface type and specifier.
interface status	Status of the interface.
HTTP Redirect Url	Url to which a subscriber's initial web browser session is redirected

Table 26: show ip interface Output Fields *(continued)*

Field Name	Field Description
line protocol	Status of the line protocol.
Description	Text description or alias if configured for the interface
Link up/down trap	Status of SNMP link up/down traps on the interface
Internet Address	IP address of the interface
IP Statistics Rcvd	
local destination	Frames with this router as destination
hdr errors	Number of packets containing header errors
addr errors	Number of packets containing addressing errors
unkn proto	Number of packets received containing unknown protocols
discards	Number of discarded packets
IP Statistics Frags	
reasm ok	Number of reassembled packets
reasm req	Number of requests for reassembly
reasm fails	Number of reassembly failures
frag ok	Number of packets fragmented successfully
frag req	Number of frames requiring fragmentation
frag fails	Number of packets unsuccessfully fragmented
IP Statistics Sent	
generated	Number of packets generated
no routes	Number of packets that could not be routed
discards	Number of packets that could not be routed and were discarded
ICMP Statistics Rcvd	
errors	Error packets received

Table 26: show ip interface Output Fields *(continued)*

Field Name	Field Description
dst unreach	Packets received with destination unreachable
time excd	Packets sent with time-to-live exceeded
param probs	Packets sent with parameter errors
src quench	Source quench packets sent
redirect	Send packets redirect
timestamp req	Requests for a timestamp
timestamp rpy	Replies to timestamp requests
addr mask req	Address mask requests
addr mask rpy	Address mask replies
ICMP Statistics Sent	
errors	Error packets received
dst unreach	Packets received with destination unreachable
time excd	Packets sent with time-to-live exceeded
param probs	Packets sent with parameter errors
src quench	Source quench packets sent
redirect	Send packets redirect
timestamp req	Requests for a timestamp
timestamp rpy	Replies to timestamp requests
addr mask req	Address mask requests
addr mask rpy	Address mask replies
ARP spoof checking	Status of the check for spoofed ARP packets received on an IP interface. Possible states: enabled or disabled. NOTE: This field is not displayed when you use the **detail** keyword.

Table 26: show ip interface Output Fields *(continued)*

Field Name	Field Description
In Received Packets, Bytes	Total number of packets and bytes received on the IP interface.
Unicast Packets, Bytes	Unicast packets and bytes received on the IP interface; link-local received multi-cast packets (non-multicast-routed frames) are counted as unicast packets.
Multicast Packets, Bytes	Multicast packets and bytes received on the IP interface which are then multicast-routed are counted as multicast packets.
In Forwarded Packets, Bytes	Packets and bytes forwarded into an output IP interface
In Total Dropped Packets, Bytes	Total number of packets and bytes that were dropped on the interface
In Policed Packets	Packets discarded on a receive IP interface for any of the following reasons: exceeding the token bucket limit, exceeding the rate limit, a drop action in a policy, discarded MAC validation packets, a destination address lookup failure or when the destination address is an IP interface that has a route configured to the null interface.
In Invalid Source Address Packets	Packets discarded on a receive IP interface because of invalid IP source address
In Error Packets	Packets discarded on a receive IP interface because of IP header errors
In Discarded Packets	Packets discarded on the ingress interface because of a configuration problem rather than a problem with the packet itself
In Fabric Dropped Packets	Packets discarded on a receive IP interface because eof internal fabric congestion
Out Forwarded Packets, Bytes	Total number of packets and bytes forwarded out of the IP interface
Unicast Packets, Bytes	Unicast packets and bytes forwarded out of the IP interface
Multicast Routed Packets, Bytes	Multicast packets and bytes forwarded out of the IP interface
Out Requested Packets, Bytes	Packets and bytes requested to be forwarded out an IP interface

Table 26: show ip interface Output Fields *(continued)*

Field Name	Field Description
Out Total Dropped Packets, Bytes	Total number of packets and bytes that were discarded on the egress interface
Out Scheduler Drops Committed Packets, Bytes	Packets and bytes dropped by the scheduler even though they had a committed traffic contract
Out Scheduler Drops Conformed Packets, Bytes	Packets and bytes dropped by the scheduler even though they conformed to the traffic contract
Out Scheduler Drops Exceeded Packets, Bytes	Packets and bytes dropped by the scheduler because they exceeded the contract
Out Policed Packets	Packets discarded on the egress interface because of rate limiting
Out Discarded Packets	Packets discarded on the egress interface because of a configuration problem rather than a problem with the packet itself
Out Fabric Dropped Packets	Packets dropped because of internal fabric congestion

Table 27 on page 151 lists the **show ipv6 interface** command output fields.

Table 27: show ipv6 interface Output Fields

Field Name	Field Description
Description	Text description or alias if configured for the interface
HTTP Redirect Url	Url to which a subscriber's initial web browser session is redirected
Internet Address	IP address of the interface
Link local address	Local IPv6 address of this interface
Network Protocols	Network protocols configured on this interface
IPv6 Statistics Rcvd	
local destination	Frames with this router as destination
hdr errors	Number of packets containing header errors
addr errors	Number of packets containing addressing errors
unkn proto	Number of packets received containing unknown protocols

Table 27: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
discards	Number of discarded packets
IP Statistics Sent	
generated	Number of packets generated
no routes	Number of packets that could not be routed
discards	Number of packets that could not be routed and were discarded
ICMPv6 Statistics Rcvd	
total	Total number of received packets
errors	Error packets received
destination unreach	Packets received with destination unreachable
admin unreach	Packets received because the destination was administratively unreachable (for example, the packet encountered a firewall filter)
param probs	Packets sent with parameter errors
time excd	Packets sent with time-to-live exceeded
pkt too big	Number of packet-too-big messages received that indicate a packet was too large to forward because of the allowed MTU size
redirects	Received packet redirects
echo requests	Echo request (ping) packets
echo replies	Echo replies received
rtr solicits	Number of received router solicitations
rtr advertisements	Number of received router advertisements
neighbor solicits	Number of received neighbor solicitations
neighbor advertisements	Number of received neighbor advertisements
Group membership (queries, responses, reductions)	Number of queries, responses, and reduction requests received from within a group to which the interface is assigned

Table 27: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
ICMPv6 Statistics Sent	
total	Total number of received packets
errors	Error packets received
destination unreach	Packets received with destination unreachable
admin unreach	Packets received because the destination was administratively unreachable (for example, the packet encountered a firewall filter)
param probs	Packets sent with parameter errors
time excd	Packets sent with time-to-live exceeded
pkt too big	Number of packet-too-big messages received that indicate a packet was too large to forward because of the allowed MTU size
redirects	Received packet redirects
echo requests	Echo request (ping) packets
echo replies	Echo replies received
rtr solicits	Number of received router solicitations
rtr advertisements	Number of received router advertisements
neighbor solicits	Number of received neighbor solicitations
neighbor advertisements	Number of received neighbor advertisements
Group membership (queries, responses, reductions)	Number of queries, responses, and reduction requests received from within a group to which the interface is assigned
Operational MTU	Value of the MTU
Administrative MTU	Value of the MTU if it has been administratively overridden using the configuration
Operational speed	Speed of the interface
Administrative speed	Value of the speed if it has been administratively overridden using the configuration

Table 27: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
Creation type	Method by which the interface was created (static or dynamic)
ND reachable time	Amount of time (in milliseconds) that the neighbor is expected to remain reachable
ND duplicate address detection attempts	Number of times that the router attempts to determine a duplicate address
ND neighbor solicitation retransmission interval	Interval in which the router retransmits neighbor solicitations
ND proxy	Indicates whether the router will reply to solicitations on behalf of a known neighbor
ND RA source link layer	Indicates whether the RA includes the link layer
ND RA interval	Interval (in seconds) of the neighbor discovery router advertisement
ND RA lifetime	Lifetime (in seconds) of the neighbor discovery router advertisement
ND RA managed flag	State of the neighbor discovery router advertisement managed flag
ND RA other config flag	State of the neighbor discovery router advertisement other config flag
ND RA advertising prefixes	Configured advertisement prefixes for neighbor discovery router advertisement
In Received Packets, Bytes	Total number of packets and bytes received on the IP interface.
Unicast Packets, Bytes	Unicast packets and bytes received on the IP interface; link-local received multi-cast packets (non-multicast-routed frames) are counted as unicast packets.
Multicast Packets, Bytes	Multicast packets and bytes received on the IP interface which are then multicast-routed are counted as multicast packets.
In Total Dropped Packets, Bytes	Total number of packets and bytes that were dropped on the interface

Table 27: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
In Policed Packets	Packets discarded on a receive IP interface for any of the following reasons: exceeding the token bucket limit, exceeding the rate limit, a drop action in a policy, discarded MAC validation packets, a destination address lookup failure or when the destination address is an IP interface that has a route configured to the null interface.
In Invalid Source Address Packets	Packets discarded on a receive IP interface because of invalid IP source address
In Error Packets	Packets discarded on a receive IP interface because of IP header errors
In Discarded Packets	Packets discarded on the ingress interface because of a configuration problem rather than a problem with the packet itself
Out Forwarded Packets, Bytes	Total number of packets and bytes forwarded out of the IP interface
Unicast Packets, Bytes	Unicast packets and bytes forwarded out of the IP interface
Multicast Routed Packets, Bytes	Multicast packets and bytes forwarded out of the IP interface
Out Total Dropped Packets, Bytes	Total number of packets and bytes that were discarded on the egress interface
Out Scheduler Dropped Packets, Bytes	Number of outbound packets and bytes dropped by the scheduler
Out Policed Packets	Packets discarded on the egress interface because of rate limiting
Out Discarded Packets	Packets discarded on the egress interface because of a configuration problem rather than a problem with the packet itself
IPv6 policy	Type (input, output, local-input) and name of policy
rate-limit-profile	Name of profile
classifier-group entry	Entry index
Committed	Number of packets and bytes conforming to the committed access rate

Table 27: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
Conformed	Number of packets and bytes that exceed the committed access rate but conform to the peak access rate
Exceeded	Number of packets and bytes exceeding the peak access rate
queue, traffic class, bound to ipv6	Queue and traffic class bound to the specified IPv6 interface
Queue length	Number of bytes in queue
Dropped committed packets, bytes	Total number of committed packets and bytes dropped by this interface
Dropped conformed packets, bytes	Total number of conformed packets and bytes dropped by this interface
Dropped exceeded packets, bytes	Total number of exceeded packets and bytes dropped by this interface

Related Documentation

- show ip interface on page 175
- show ipv6 interface on page 176

Monitoring Profiles for Service Manager

Purpose Display information about the policies and QoS configurations referenced in profiles.

Action To display information about a specific profile:

```
host1#show profile name video
IP Output Policy           : video statistics disabled
IP Secondary Input Policy  : video statistics disabled
qos-parameter vidburst 1000
qos-parameter vidrate 500000
qos-profile vid512k
```

```
host1#show profile name foo

IP Policy Parameter foo : 100000 increase, reference rate
IP Input Policy            : p1 statistics disabled

ERX-00-16-c2#show profile name p2

IP Policy Parameter foo : 100000, reference rate
IP Input Policy            : p1 statistics disabled
```

To display a list of profiles configured on the router:

```
host1#show profile brief
```

Meaning Table 28 on page 157 lists the **show profile** command output fields.

Table 28: show profile Output Fields

Field Name	Field Description
Input Policy	Name of input policy and whether statistics are enabled or disabled
Output Policy	Name of output policy and whether statistics are enabled or disabled
qos-parameter	Name and value of the QoS parameter assigned to the profile
qos-profile	Name of the QoS profile assigned to the profile

Related Documentation

- show profile on page 171

Monitoring Service Definitions

Purpose Display information about the service definitions configured on your router.

Action To display information for the particular service definition, specify the name of a service definition macro file, including the .mac extension:

```
host1#show service-management service-definition tiered.mac
tiered.mac - WED DEC 14 14:41:20 2005
 Installed: True
 Service: tiered(inputbw, outputbw)
 Reference Count: 0
```

To display summary information for all service definitions:

```
host1#show service-management service-definition brief
                      Service Definitions
                      -------------------
                                                          Reference
 Filename             Service             Installed        Count
----------   -------------------------   ---------   ---------
video.mac    video(inputbw, outputbw)    True        0
tiered.mac   tiered(inputbw, outputbw)   True        0

 Filename            Timestamp
----------   ------------------------
video.mac    TUE NOV 15 15:22:00 2005
tiered.mac   WED DEC 14 14:41:20 2005
```

Meaning Table 29 on page 158 lists the **show service-management service-definition** command output fields.

Table 29: show service-management service-definition Output Fields

Field Name	Field Description
Filename	Name of the service definition macro file
Service	Name of the service, with the parameter specifications in parentheses
Installed	Status of definition: • True—installed • False—not installed
Reference Count	Number of times the service definition has been used to instantiate a unique service instance (which identifies the policy, QoS, and profile objects for a service). For example, if one service session—such as, tiered(40000,40000)—is activated by multiple subscribers, the reference count is 1. However, if one subscriber activates tiered(40000,40000) and another subscriber activates tiered(75000,75000)—the reference count is 2.
Timestamp	Day, date, and time the service definition was copied to NVS.

Related Documentation

- show service-management service-definition on page 177

Monitoring Service Session Profiles

Purpose Display information about service session profiles configured on your router.

Action To display summary information for all service session profiles:

```
host1#show service-management service-session-profile brief
    Service Session Profiles
    ------------------------
Name      Volume   Time   Statistics
-------   ------   ----   ----------
tiered1   20000    1000   Volume-Time
tiered2   20000    1000   Time
video1    15000    1000   Volume-Time
video4    0        0      Disabled
```

To display information for a particular service session profile:

```
host1#show service-management service-session-profile tiered1
tiered1
 Time       : 1000
 Volume     : 20000
 Statistics : Time and Volume
```

Meaning Table 30 on page 159 lists the **show service-management service-session-profile** command output fields.

Table 30: show service-management service-session-profile Output Fields

Field Name	Field Description
Name	Name of the service session profile
Volume	Volume threshold, in MB, for the service session
Time	Time threshold, in seconds, for the service session
Statistics	Type of statistics that are captured: • Disabled (none) • Time • Volume–Time • Time and Volume

Related Documentation

- show service-management service-session-profile on page 178

CHAPTER 25

Monitoring Service and Subscriber Sessions

Monitoring Active Subscriber Sessions with Service Manager

Purpose Display information about active subscriber sessions on your router.

Action To display summary information for all active subscriber sessions:

```
host1# show service-management subscriber-session brief
                          Subscriber Sessions
                          -------------------
                                                                    Service
     Name          Interface       Id   Owner/Id      State    Non-volatile  Sessions
----------------   -------------   --   ---------     ------   ------------  --------
CLIENT1@ISP.COM    ip192.168.0.3   1    AAA 4194326   Active   False         1
CLIENT2@ISP.COM    ip192.168.0.7   2    AAA 4194327   Active   False         1
CLIENT3@ISP.COM    ip192.168.0.4   3    AAA 4194328   Active   False         1
CLIENT4@ISP.COM    ip192.168.0.5   4    AAA 4194329   Active   False         1
CLIENT5@ISP.COM    ip192.168.0.6   5    AAA 4194330   Active   False         1
CLIENT6@ISP.COM    ip192.168.0.8   6    AAA 4194331   Active   False         1
CLIENT7@ISP.COM    ip192.168.0.1   7    AAA 4194332   Active   False         1
CLIENT8@ISP.COM    ip192.168.0.9   8    AAA 4194333   Active   False         1
CLIENT9@ISP.COM    ip192.168.0.2   9    AAA 4194334   Active   False         1
CLIENT10@ISP.COM   ip192.168.0.10  10   AAA 4194335   Active   False         1
```

To display information for that particular subscriber with the subscriber name:

```
host1# show service-management subscriber-session client1@isp.com interface ip 192.168.0.1
User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1
 Id: 1
 Owner: AAA 4194326
 Non-volatile: False
 State: Active
 ServiceSessions:
         Name             mutex   Owner/Id      State                Operation
-----------------------   -----   -----------   ------------------   ---------
tiered(2000000,3000000)           AAA 4194326   ConfigApplySuccess   Activate
         Name             Non-volatile
```

```
----------------------   ------------
tiered(2000000,3000000)   False
```

To display information for that particular subscriber with the service session:

```
host1#  show service-management subscriber-session client1@isp.COM interface ip 192.168.0.1
 service-session tiered
User Name: client1@isp.COM, Interface: ip192.168.0.1
Service : tiered(2000000,3000000)
 Non-volatile : False
 Owner : AAA 41943236
 State : Config ApplySuccess
 Activate : True
 Statistics Type : time-based and volume-based
 Statistics Complete : False
 Poll Interval : 0
 Poll Expire : 0
 Activate Time : THU MAR 02 01:21:26 2006
 Time : 0
 Time Expire : 0
 Volume MBytes: 2
 Volume Expire MBytes : 1
 Input Bytes : 594
 Output Bytes : 1196
 Input Packets : 1
 Output Packets : 2
```

To display information for a particular subscriber using the subscriber ID:

```
host1#show service-management subscriber-session 20

User Name: CLIENT50@ISP.COM, Interface: ip192.168.100.33
 Id: 20
 Owner/Id: CLI
 Non-volatile: True
 State: Active
 ServiceSessions:
      Name            mutex   Owner   State                Operation
------------------   -----   -----   ------------------   ---------
internet(5000,8000)      12   CLI     Config ApplySuccess   Activate

      Name            Non-volatile
------------------    ------------
internet(5000,8000)   True
```

Meaning Table 31 on page 162 lists the **show service-management subscriber-session** command output fields.

Table 31: show service-management subscriber-session Output Fields

Field Name	Field Description
Name	Name of the subscriber or name of the service session
Interface	Type and IP address of the subscriber's interface
Id	ID number of the subscriber session
mutex	Index number of the mutex group to which the service session belongs

Table 31: show service-management subscriber-session Output Fields *(continued)*

Field Name	Field Description
Owner/Id	Method used to activate the subscriber session (CLI, AAA) and ID number generated by the owner (Acct-Session-ID for AAA)
State	Status of the subscriber session (active or inactive), or status of the service session
Non-volatile	Indicates whether the service session is stored in NVS; RADIUS-based service sessions are not stored in NVS
Service Sessions	Number of service sessions currently active for this subscriber
Operation	Last operation that Service Manager performed
Service	Name of the service, with parameter values in parentheses
Activate	Indicates whether the last operation was activate (True) or deactivate (False)
Statistics Type	Type of statistics collected; none, time, or volume-time
Statistics Complete	Whether statistics have been successfully collected; True or False
Poll Interval	Interval, in seconds, that interim statistics reports are sent
Poll Expire	Number of seconds until the next statistics report is sent
Activate Time	Day, date, and time when the service session was activated
Time	Time threshold value set by service session profile or RADIUS VSA
Time Expire	Time left until the threshold expires; this value starts as the time threshold value and is decremented as time passes
Volume	Volume threshold value set by service session profile or RADIUS VSA
Volume Expire	Volume left until the threshold is exceeded; this value starts as the volume threshold value and is decremented as the service statistics measure volume

Table 31: show service-management subscriber-session Output Fields *(continued)*

Field Name	Field Description
Input Bytes	Current value of input bytes that the statistics configuration is measuring
Output Bytes	Current value of output bytes that the statistics configuration is measuring
Input Packets	Current value of input packets that the statistics configuration is measuring
Output Packets	Current value of output packets that the statistics configuration is measuring

Related Documentation

- show service-management subscriber-session on page 180

Monitoring Active Owner Sessions with Service Manager

Purpose Display information about active subscriber sessions, by owner.

Action To display summary information for all active owner sessions:

```
host1# show service-management owner-session brief
                              Subscriber Sessions
                              -------------------
                                                                        Service
   Name           Interface       Id  Owner/Id     State   Non-volatile  Sessions
---------------- -------------- --  ---------    ------ ------------  --------
CLIENT1@ISP.COM   ip192.168.0.3  1  AAA 4194326  Active  False         1
CLIENT2@ISP.COM   ip192.168.0.7  2  AAA 4194327  Active  False         1
CLIENT3@ISP.COM   ip192.168.0.4  3  AAA 4194328  Active  False         1
CLIENT4@ISP.COM   ip192.168.0.5  4  AAA 4194329  Active  False         1
CLIENT5@ISP.COM   ip192.168.0.6  5  AAA 4194330  Active  False         1
CLIENT6@ISP.COM   ip192.168.0.8  6  AAA 4194331  Active  False         1
CLIENT7@ISP.COM   ip192.168.0.1  7  AAA 4194332  Active  False         1
CLIENT8@ISP.COM   ip192.168.0.9  8  AAA 4194333  Active  False         1
```

To display information for a particular owner:

```
host1# show service-management owner-session aaa 4194326
User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1
 Owner/Id: AAA/4194326
 Non-volatile: False
 State: Active
 ServiceSessions:
         Name             Owner/ID      State                 Operation
-----------------------   -----------   -------------------   ---------
tiered(2000000,3000000)   AAA 4194326   Config ApplySuccess   Activate
         Name             Non-volatile
-----------------------   ------------
tiered(2000000,3000000)   False
```

To display information for a particular owner with service session information:

```
host1# show service-management owner-session aaa 4194326 service-session
User Name: client1@isp.COM, Interface: ip192.168.0.1
Service : tiered(2000000,3000000)
 Non-volatile : False
 Owner : AAA 4194326
 State : Config ApplySuccess
 Activate : True
 Statistics Type : time-based and volume-based
 Statistics Complete : False
 Poll Interval : 0
 Poll Expire : 0
 Activate Time : THU MAR 02 01:21:26 2006
 Time : 0
 Time Expire : 0
 Volume MBytes: 2
 Volume Expire MBytes : 1
 Input Bytes : 594
 Output Bytes : 1196
 Input Packets : 1
 Output Packets : 2
```

Meaning Table 32 on page 165 lists the **show service-management owner-session** command output fields.

Table 32: show service-management owner-session Output Fields

Field Name	Field Description
Name	Name of the subscriber or name of the service session
Interface	Type and IP address of the subscriber's interface
Owner/Id	Method used to activate the subscriber session (CLI, AAA) and ID number generated by the owner
State	Status of the subscriber session (active or inactive), or status of the service session
Non-volatile	Indicates whether the service session is stored in NVS; RADIUS-based service sessions are not stored in NVS
Service Sessions	Number of service sessions currently active for this subscriber
Operation	Last operation that Service Manager performed
Service	Name of the service, with parameter values in parentheses
Activate	Indicates whether the last operation was activate (True) or deactivate (False)
Statistics Type	Type of statistics collected; none, time, or volume-time

Table 32: show service-management owner-session Output Fields *(continued)*

Field Name	Field Description
Statistics Complete	Whether statistics have been successfully collected; True or False
Poll Interval	Interval, in seconds, that interim statistics reports are sent
Poll Expire	Number of seconds until the next statistics report is sent
Activate Time	Day, date, and time when the service session was activated
Time	Time threshold value set by service session profile or RADIUS VSA
Time Expire	Time left until the threshold expires; this value starts as the time threshold value and is decremented as time passes
Volume	Volume threshold value set by service session profile or RADIUS VSA
Volume Expire	Volume left until the threshold is exceeded; this value starts as the volume threshold value and is decremented as the service statistics measure volume
Input Bytes	Current value of input bytes that the statistics configuration is measuring
Output Bytes	Current value of output bytes that the statistics configuration is measuring
Input Packets	Current value of input packets that the statistics configuration is measuring
Output Packets	Current value of output packets that the statistics configuration is measuring

Related Documentation

- show service-management owner-session on page 179

Monitoring the Number of Active Subscriber and Service Sessions with Service Manager

Purpose Display the total number of active subscriber and service sessions configured on your router.

Action To display the total number of active subscriber and service sessions:

```
host1#show service-management summary
Total Subscriber Sessions : 10
Total Service Sessions : 10
```

Meaning Table 33 on page 167 lists the **show service-management summary** command output fields.

Table 33: show service-management summary Output Fields

Field Name	Field Description
Total Subscriber Sessions	Number of active subscriber sessions on the router
Total Service Sessions	Number of active service sessions on the router

Related Documentation

- show service-management summary on page 181

CHAPTER 26

Monitoring Commands

show ip http

Syntax show ip http [scalar | server | statistics [delta]] [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information about HTTP local servers, information about the parameters configured for the HTTP local server, and statistics about the connections to the HTTP local server.

Options

- scalar—Displays information about the connections to the HTTP local server
- server—Displays information about the parameters configured for the HTTP local server
- statistics—Display statistics about the connections to the HTTP local server
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec

Related Documentation

- Monitoring the Configuration of the HTTP Local Server on page 141

show profile

Syntax show profile name *profileName* [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about a specific IP profile, such as the available PPPoE profile information: PPPoE URL string, PPPoE MOTM string, or both. If neither exists, the fields do not appear in the display.

Options
- *profileName*—Name of the profile
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show aaa service accounting interval

Syntax show aaa service accounting interval [*filter*]

Release Information Command introduced in JunosE Release 9.0.0.

Description Displays the default accounting interval used by the Service Manager application for RADIUS-initiated services associated with users attached to this virtual router.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show license

Syntax show license [*licenseType*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
service-management keyword added in JunosE Release 7.2.0.

Description Displays all licenses or a specified license.

NOTE: The **show license l2tp-session** command remains in the CLI even though a separate L2TP license is no longer required to enable support for 32,000 L2TP sessions on supported systems.

Options
- *licenseType*—bfd, b-ras, ipsec-tunnels, ipv6, l2tp-session, nat, or service-management
- *filter*—See Filtering show Commands

Mode Privileged Exec

show profile

Syntax show profile name *profileName* [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about a specific IP profile, such as the available PPPoE profile information: PPPoE URL string, PPPoE MOTM string, or both. If neither exists, the fields do not appear in the display.

Options
- *profileName*—Name of the profile
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show ip interface

Syntax show ip interface [vrf *vrfName*]
{ { [brief | detail | other | show-virtual-router [*virtualRouterName*]]
[*interfaceType interfaceSpecifier*] } | summary } [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
show-virtual-router keyword and *virtualRouterName* variable added in JunosE Release 7.3.0.
other keyword added in JunosE Release 8.0.0.

Description Displays current state of all IP interfaces or the IP interfaces you specify. The default is all interface types and all interfaces.

Options
- *vrfName*—Name of the VRF
- brief—Displays a brief summary of IP status and configuration information
- detail—Shows a detailed display of IP status and configuration information
- other—Shows hidden interfaces and routes to the local address that are used internally so that from a given CE you can now ping the local address of any VRF that has a VPN overlapping a VPN to which the CE belongs
- *virtualRouterName*—Name of the virtual router
- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
- summary—Shows a detailed summary of IP status and configuration
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring the QoS Configuration of IP Interfaces
- Monitoring the Policy Configuration of IP Interfaces
- Monitoring the Packet Mirroring Configuration of IP Interfaces

show ipv6 interface

Syntax

show ipv6 interface [vrf *vrfName*] [brief | detail]
[*interfaceType interfaceSpecifier*][delta] [*filter*]

To display summary information:

show ipv6 interface summary [vrf *vrfName*] [*filter*]

Release Information

Command introduced before JunosE Release 7.1.0.
vrf keyword and *vrfName* variable added in JunosE Release 7.2.0.

Description

Displays current state of all IPv6 interfaces or the IPv6 interfaces that you specify. The default is all interface types and all interfaces.

Options

- *vrfName*—Name of the VRF
- brief—Displays a brief summary of IPv6 status and configuration information
- detail—Shows a detailed display of IP status and configuration information
- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands
- summary—Shows a detailed summary of IP status and configuration

Mode

Privileged Exec, User Exec

Related Documentation

- Monitoring the Policy Configuration of IPv6 Interfaces

show service-management service-definition

Syntax show service-management service-definition { *fileName*.mac | brief } [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information for all service definitions or for the specified service definition.

Options
- *fileName*—Name of the service definition macro file
- brief—Displays limited information about the service definitions
- *filter*—See Filtering show Commands

Mode Privileged Exec

show service-management service-session-profile

Syntax show service-management service-session-profile { *profileName* | brief } [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information for user sessions.

Options
- *profileName*—Name of the service session profile
- brief—Displays limited information about the user sessions
- *filter*—See Filtering show Commands

Mode Privileged Exec

show service-management owner-session

Syntax show service-management owner-session { brief | *subscriberId* | *ownerName ownerId* [service-session *serviceName*] } [*filter*]

Release Information Command introduced in JunosE Release 8.0.0.

Description Displays subscriber session information based on the session owner.

Options

- brief—Displays limited information about the owner sessions
- *subscriberId*—ID of the subscriber
- *ownerName*—Name of the owner for the owner session; AAA for RADIUS-based subscribers
- *ownerId*—Unique ID of the owner for the owner session; Acct-Session-ID for RADIUS-based subscribers
- *serviceName*—Name of the service session used for the owner session
- *filter*—See Filtering show Commands

Mode Privileged Exec

show service-management subscriber-session

Syntax show service-management subscriber-session { brief | *subscriberId* | *subscriberName* [interface *interfaceType interfaceSpecifier* [service-session *serviceName*]] } [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information for subscriber sessions.

Options

- brief—Displays limited information about the user sessions
- *subscriberId*—ID of the subscriber
- *subscriberName*—Name of the subscriber
- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers
- *serviceName*—Name of the service session used for the subscriber session
- *filter*—See Filtering show Commands

Mode Privileged Exec

show service-management summary

Syntax show service-management summary [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays summary information for all subscriber and service sessions.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

PART 4

Index

Index

P

Q

R

S

T