JUNIPER NETWORKS

Junos® OS

AAA Service Framework Feature Guide for Subscriber Management

Release
13.2

Published: 2013-07-31

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

Junos® OS AAA Service Framework Feature Guide for Subscriber Management
13.2

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

Documentation and 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/.

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version (if applicable)

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

AAA Services in Subscriber Access Networks

AAA Service Framework Overview

The authentication, authorization, and accounting (AAA) Service Framework provides a single point of contact for all the authentication, authorization, accounting, address assignment, and dynamic request services that the router supports for network access.

The framework supports authentication and authorization through external servers, such as RADIUS. The framework also supports accounting and dynamic-request change of authorization (CoA) and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS.

When interacting with external back-end RADIUS servers, the AAA Service Framework supports standard RADIUS attributes and Juniper Networks vendor specific attributes (VSAs). The AAA Service Framework also includes an integrated RADIUS client that is compatible with RADIUS servers that conform to RFC-2865, *Remote Authentication Dial In User Service (RADIUS)*, RFC-2866, *RADIUS Accounting*, and RFC-3576, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*, and which can initiate requests.

You create the following types of configurations to manage subscriber access.

- Authentication—Authentication parameters defined in the access profile determine the authentication component of the AAA processing. For example, subscribers can be authenticated using an external authentication service such as RADIUS.
- Accounting—Accounting parameters in the access profile specify the accounting part of the AAA processing. For example, the parameters determine how the router collects and uses subscriber statistics. You can also configure AAA to enable the router to collect statistics on a per-service session basis for subscribers.
- RADIUS-initiated dynamic requests—A list of authentication server IP addresses in the access profile specify the RADIUS servers that can initiate dynamic requests to the router. Dynamic requests include CoA requests, which specify VSA modifications and service changes, and disconnect requests, which terminate subscriber sessions. The list of authentication servers also provide RADIUS-based dynamic service activation and deactivation during subscriber login.
- Address assignment—The AAA Service Framework assigns addresses to subscribers based on the configuration of local address-assignment pools. For example, the AAA framework collaborates with RADIUS servers to assign addresses from the specified pools.
- Subscriber secure policy—RADIUS VSAs and attributes provide RADIUS-initiated traffic mirroring on a per-subscriber basis.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- RADIUS Acct-On and Acct-Off Messages on page 25
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- *Address-Assignment Pools Overview*
- DNS Address Assignment Precedence on page 9
- RADIUS Accounting Statistics for Subscriber Access Overview on page 19
- Using RADIUS Dynamic Requests for Subscriber Access Management on page 31
- *Subscriber Secure Policy Overview*

RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework

The AAA Service Framework supports RADIUS attributes and vendor-specific attributes (VSAs). This support provides tunable parameters that the subscriber access management feature uses when creating subscribers and services.

RADIUS attributes are carried as part of standard RADIUS request and reply messages. The subscriber management access feature uses the RADIUS attributes to exchange specific authentication, authorization, and accounting information. VSAs allow the subscriber access management feature to pass implementation-specific information that provide extended capabilities, such as service activation or deactivation, and enabling and disabling filters.

When you use dynamic profiles, the AAA Service Framework supports the use of Junos OS predefined variables to specify the RADIUS attribute or VSA for the information obtained from the RADIUS server.

Related Documentation

- RADIUS IETF Attributes Supported by the AAA Service Framework on page 37
- Juniper Networks VSAs Supported by the AAA Service Framework on page 44
- DSL Forum Vendor-Specific Attributes on page 63
- AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 54
- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 59
- Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 66

RADIUS Server Options for Subscriber Access

You can specify options that the router uses when communicating with RADIUS authentication and accounting servers for subscriber access.

The following list describes the RADIUS options you can configure:

- **accounting-session-id-format**—The format the router uses to identify the accounting session. The identifier can be in one of the following formats. The router uses **decimal** format by default.
  - **decimal**—For example, **435264**
  - **description**—In the format, **jnpr interface-specifier:subscriber-session-id**. For example, **jnpr fastEthernet 3/2.6:1010101010101**
- **calling-station-id-delimiter**—The character that the router uses as the separator between concatenated values in the Calling-Station-ID string (RADIUS attribute 31).

- **calling-station-id-format**—Optional information that the router includes in the Calling-Station-ID (RADIUS attribute 31).
- **client-accounting-algorithm** and **client-authentication-algorithm**—The method the router uses to access RADIUS accounting and RADIUS authentication servers. You can specify the following methods:
  - **direct**—The default method, in which there is no load balancing. For example, in the direct method, the router always accesses **server1** (the primary server) first, and uses **server2** and **server3** as backup servers.
  - **round-robin**—The method that provides load balancing by rotating router requests among the list of configured RADIUS servers. For example, if three RADIUS servers are configured to support the router, the router sends the first request to **server1**, and uses **server2** and **server3** as backup servers. The router then sends the second request to **server2**, and uses **server3** and **server1** as backups.

NOTE: When a RADIUS server in the round-robin list becomes unreachable, the next reachable server in the round-robin list is used for the current request. That same server is also used for the next request because it is at the top of the list of available servers. As a result, after a server failure, the server that is used takes up the load of two servers.

- **coa-dynamic-variable-validation**—The optional method that the router uses when processing CoA requests that include changes to a client profile dynamic variable that cannot be applied. The optional configuration specifies that when a CoA operation is unable to apply a requested change to a client profile dynamic variable, subscriber management does not apply any changes to client profile dynamic variables in the CoA request and then responds with a NACK. In the default method, subscriber management does not apply the incorrect update but does apply the other changes to the client profile dynamic variables, and then responds with an ACK message.
- **access-loop-id-local**—The Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database. The interface description of the logical interface is used as the Agent-Remote-Id and the interface description portion of the NAS-Port-Id using the format **<underlying-interface-name>:<outer-tag>-<inner-tag>** is used as the Agent-Circuit-Id.

NOTE: The NAS-Port-Id format changes (established by **[set access profile *profile-name* radius options interface-description-format]**) are applied before generating the Agent-Circuit-Id.

The NAS-Port-Id format (established by **[set access profile *profile-name* radius options interface-description-format]**) leverages the locally generated Agent-Remote-Id and Agent-Circuit-Id.

- **ethernet-port-type-virtual**—The physical port type of **virtual** that the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). By default the router passes a port type of **ethernet** in RADIUS attribute 61.
- **interface-description-format**—The information that is excluded from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the **subinterface** and the **adapter** in the interface description. You can specify:
  - **exclude-adapter**—Exclude the adapter.
  - **exclude-subinterface**—Exclude the subinterface.
- **nas-identifier**—The value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests. You can specify a string in the range 1 through 64 characters.
- **nas-port-extended-format**—The extended format for RADIUS attribute 5 (NAS-Port) and for the width of the fields in the NAS-Port attribute that the RADIUS client uses. You can specify:
  - **adapter-width *width***—Number of bits in the adapter field.
  - **port-width *width***—Number of bits in the port field.
  - **slot-width *width***—Number of bits in the slot field.
  - **stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
  - **vlan-width *width***—Number of bits in the VLAN ID field.

NOTE: **The total of the widths must not exceed 32 bits, or the configuration will fail.**

You can configure an extended format for the NAS-Port attribute for both Ethernet subscribers and ATM subscribers. For ATM subscribers, you can specify:

- **adapter-width**—Number of bits in the ATM adapter field, in the range 1 through 32
- **port-width**—Number of bits in the ATM port field, in the range 1 through 32
- **slot-width**—Number of bits in the ATM slot field, in the range 1 through 32
- **vpi-width**—Number of bits in the ATM virtual path identifier (VPI) field, in the range 1 through 32
- **vci-width**—Number of bits in the ATM virtual circuit identifier (VCI) field, in the range 1 through 32

NOTE: **For ATM subscribers, the combined total of the widths of all fields must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.**

- **nas-port-id-delimiter**—The character used as the separator between values in the NAS-Port-ID string.
- **nas-port-id-format**—Optional information included in RADIUS attribute 87 (NAS-Port-ID).
- **nas-port-type**—The port type used to authenticate subscribers.
- **revert-interval**—The number of seconds that the router waits after a server has become unreachable. The router rechecks the connection to the server when the **revert-interval** expires. If the server is then reachable, it is used in accordance with the order of the server list. You can configure from 0 (off) through 604800 seconds. The default is 60 seconds.
- **vlan-nas-port-stacked-format**—The format that turns off RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118

Global RADIUS Options for Subscriber Access

You can specify options that the router uses when communicating with all configured RADIUS servers for subscriber access.

The following list describes the global RADIUS options you can configure:

- **revert-interval**—The number of seconds that the router waits after a server has become unreachable. The router rechecks the connection to the server when the **revert-interval** expires. If the server is then reachable, it is used in accordance with the order of the server list. You can configure from 0 (off) through 604800 seconds. The default is 60 seconds.
- **request-rate**—The number of requests per second that the router can send to all configured RADIUS servers collectively. By limiting the flow of requests from the router to the RADIUS servers, you can prevent the RADIUS servers from being flooded with requests. You can configure from 500 through 4000 requests per second. The default is 500 requests per second.

Related Documentation

- Configuring RADIUS Options for Subscriber Access Globally on page 121
- request-rate on page 241
- revert-interval on page 243

Retaining Authentication and Accounting Information During Session Startup

At subscriber session startup, the Junos OS **authd** process sends an Acct-On message to the RADIUS server and the new session starts authentication and accounting operations. However, in some service provider environments, upon receipt of the Acct-On message, the RADIUS server cleans up the previous session state and removes accounting

statistics. In this scenario, the RADIUS server's cleanup operation can inadvertently delete the new session's authentication and accounting information, which might include customer billing information.

To ensure that the new session's authentication and accounting information is not deleted, you can optionally use the **wait-for-acct-on-ack** statement to configure the **authd** process to wait for an Acct-On-Ack response message from the RADIUS accounting server, so the RADIUS cleanup can finish before **authd** sends any new authentication and accounting updates.

You configure this feature for an access profile for a logical system and routing instance context. All authentication requests fail until the router receives an Acct-On-Ack response from a RADIUS accounting server that is configured in the access profile. If multiple RADIUS accounting servers are configured for the access profile, **authd** waits until the first response is received.

You can also configure the **authd** process to send accounting messages when the RADIUS server status changes for an access profile. This configuration enables you to monitor whether the access profile has an active RADIUS server. You use the **send-acct-status-on-config-change** statement to specify that **authd** send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is deleted from the access profile.

Related Documentation

- Configuring Per-Subscriber Session Accounting on page 110

DNS Address Assignment Precedence

Subscriber management supports three methods for assigning addresses to DHCP clients. When multiple methods are configured, the router uses the following precedence to determine which address to assign to the client.

1. Address defined on the RADIUS server by Internet Assigned Numbers Authority (IANA) vendor ID 4874 attributes 26-4 (Primary-DNS) and 26-5 (Secondary-DNS).
2. Address defined on the RADIUS server by IANA vendor ID 2636 attributes 26-31 (Primary-DNS) and 26-33 (Secondary-DNS).
3. Address defined in the local address pool on the router.

Related Documentation

- Juniper Networks VSAs Supported by the AAA Service Framework on page 44
- *Address-Assignment Pools Overview*

Manual Configuration of the NAS-Port-ID RADIUS Attribute

Subscriber management uses the NAS-Port-ID (RADIUS attribute 87) to provide an interface description that identifies the physical interface that is used to authenticate subscribers. The NAS-Port-ID is included in RADIUS Access-Request, Acct-Start, Acct-Stop, Acct-On, and Acct-Off messages.

You can configure access profiles to specify additional information in the NAS-Port-ID. The additional information can be any combination of the interface description (the default value), the Agent Circuit ID, the Agent Remote ID, and the NAS identifier. You can also specify an optional delimiter character, which separates the values in a NAS-Port-ID. The default delimiter character is the hash character (**#**).

A default NAS-Port-ID consists of the following **interface-description** string:

[physical-interface].<interface-type>-<slot>/<adapter>/<port><.subinterface>[:<svlan>-<vlan>]

For example: **ge-1/2/0.100:100**

You might optionally configure an access profile that specifies that the NAS-Port-ID includes the NAS identifier, the Agent Circuit ID, and the Agent Remote ID, in addition to the default interface description. For this configuration, the NAS-Port-ID consists of the following string:

nas-identifier#interface-description#agent-circuit-id#agent-remote-id

For example:

retailer25#ge-1/2/0.100:100#ACI 12/1/22/1230:1.1.23#ARI 55/2/23.9999:10.11.1923

NOTE: The NAS-Port-ID displays the configured values in the following order (where # is the delimiter):

nas-identifier#interface-description#agent-circuit-id#agent-remote-id

Related Documentation

- Configuring a NAS-Port-ID with Additional Options on page 125
- RADIUS Server Options for Subscriber Access on page 5

Manual Configuration of the NAS-Port-Type RADIUS Attribute

Subscriber management uses the NAS-Port-Type (RADIUS attribute 61) to identify the type of physical port that is used to authenticate subscribers. By default, subscriber management uses a NAS-Port-Type of **ethernet**.

You can optionally configure access profiles to provide the value for the NAS-Port-Type attribute, which enables you to explicitly specify the NAS port type that is used for a given connection. For example, you might configure an access profile that specifies that a NAS port type of **wireless** is used for all Ethernet connections that are managed by that access profile.

NOTE: The **ethernet-port-type-virtual** configuration statement takes precedence over the **nas-port-type** statement when you include both statements in the same access profile. When you include the **ethernet-port-type-virtual** statement, subscriber management uses the RADIUS attribute value of **5**, which specifies a NAS port type of **virtual**.

Table 3 on page 11 shows the supported port type values for RADIUS attribute 61 (NAS-Port-Type) that you can include in an access profile.

Table 3: RADIUS NAS-Port-Type Values

Statement Option	NAS-Port-Type Value	Description
value	0–65535	Number that indicates either the IANA-assigned value for the RADIUS port type or a custom number-to-port type defined by the user
adsl-cap	12	Asymmetric DSL, carrierless amplitude phase (CAP) modulation
adsl-dmt	13	Asymmetric DSL, discrete multitone (DMT)
async	0	Asynchronous
cable	17	Cable
ethernet	15	Ethernet
fddi	21	Fiber Distributed Data Interface
g3-fax	10	G.3 Fax
hdlc-clear-channel	7	HDLC Clear Channel
iapp	25	Inter-Access Point Protocol (IAPP)
idsl	14	ISDN DSL
isdn-sync	2	ISDN Synchronous
isdn-v110	4	ISDN Async V.110
isdn-v120	3	ISDN Async V.120
piafs	6	Personal Handyphone System (PHS) Internet Access Forum Standard
sdsl	11	Symmetric DSL

Table 3: RADIUS NAS-Port-Type Values *(continued)*

Statement Option	NAS-Port-Type Value	Description
sync	1	Synchronous
token-ring	20	Token Ring
virtual	5	Virtual
wireless	18	Other wireless
wireless-1x-ev	24	Wireless 1xEV
wireless-cdma2000	22	Wireless code division multiple access (CDMA) 2000
wireless-ieee80211	19	Wireless 802.11
wireless-umts	23	Wireless universal mobile telecommunications system (UMTS)
x25	8	X.25
x75	9	X.75
xdsl	16	DSL of unknown type

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118

RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview

On MX Series routers with Modular Port Concentrator/Modular Interface Card (MPC/MIC) interfaces, you can configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-interface, per-VLAN, or per-stacked VLAN basis. The router passes the NAS-Port and NAS-Port-Type attributes to the RADIUS server during the authentication, authorization, and accounting (AAA) process.

This overview covers the following topics:

- NAS-Port-Type RADIUS Attribute on page 13
- NAS-Port RADIUS Attribute on page 13
- NAS-Port Options Configuration and Subscriber Network Access Models on page 13
- NAS-Port Options Definition on page 13

NAS-Port-Type RADIUS Attribute

The NAS-Port-Type attribute specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber. When you use the **nas-port-type** statement to configure the NAS-Port-Type, you can specify one of several predefined port types, or a user-defined port type value in the range 0 through 65535.

NAS-Port RADIUS Attribute

The NAS-Port attribute specifies the physical port number of the NAS that is authenticating the user, and is formed by a combination of the physical port's slot number, port number, adapter number, VLAN ID, and S-VLAN ID. The NAS-Port extended format, which you configure with the **nas-port-extended-format** statement, specifies the number of bits (bit width) for each field in the NAS-Port attribute: slot, adapter, port, VLAN, and S-VLAN.

To include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format, use the **stacked** option as part of the **nas-port-extended-format** statement. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.

NAS-Port Options Configuration and Subscriber Network Access Models

Configuring the NAS-Port-Type and the extended format for NAS-Port on a per-VLAN, per-stacked VLAN, or per-physical interface basis is useful in network configurations that use the following subscriber access models:

- 1:1 access model (per-VLAN basis)—In a 1:1 access model, dedicated customer VLANs (C-VLANs) provide a one-to-one correspondence between an individual subscriber and the VLAN encapsulation.
- N:1 access model (per–S-VLAN basis)—In an N:1 access model, service VLANs are dedicated to a particular service, such as video, voice, or data, instead of to a particular subscriber. Because a service VLAN is typically shared by many subscribers within the same household or in different households, the N:1 access model provides a many-to-one correspondence between individual subscribers and the VLAN encapsulation.
- 1:1 or N:1 access model (per-physical interface basis)—You can configure the NAS-Port-Type and NAS-Port format on a per-physical interface basis for both the 1:1 access model and the N:1 access model.

NAS-Port Options Definition

As an alternative to globally configuring the NAS-Port-Type and NAS-Port extended format in an access profile, you can configure these attributes on a per-interface, per-VLAN, or per-stacked VLAN basis. To do so, you must create a *NAS-Port options definition*, which includes some or all of the following components:

- NAS-Port-Type value—Specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

- NAS-Port extended format—Configures the number of bits (bit width) for each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN. Optionally, you can also use the **stacked** option as part of the **nas-port-extended-format** statement to include S-VLAN IDs, in addition to VLAN IDs, in the extended format. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.
- VLAN ranges or S-VLAN ranges—Defines the VLAN range of subscribers or stacked VLAN range of subscribers to which each NAS-Port options definition applies.

Related Documentation

- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135

Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN

The following guidelines apply when you configure the NAS-Port-Type attribute and the extended format for the NAS-Port attribute on a per-VLAN, per-stacked VLAN, or per-physical interface basis:

- You can create a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include either a maximum of 32 VLAN ranges or a maximum of 32 stacked VLAN ranges, but cannot include a combination of VLAN ranges and stacked VLAN ranges.
- Configuring the NAS-Port-Type attribute and NAS-Port extended format on a per-VLAN, per-stacked VLAN, or per-physical interface basis overrides the global settings for these attributes configured in an access profile.
- If the NAS-Port-Type attribute and the NAS-Port extended format are not configured on a per-VLAN basis (in a 1:1 access model) or on a per-stacked VLAN basis (in an N:1 access model), the router uses the global settings configured for these attributes in an access profile for all RADIUS request messages.

Related Documentation

- RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 12
- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135

Centrally Configured Opaque DHCP Options

Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

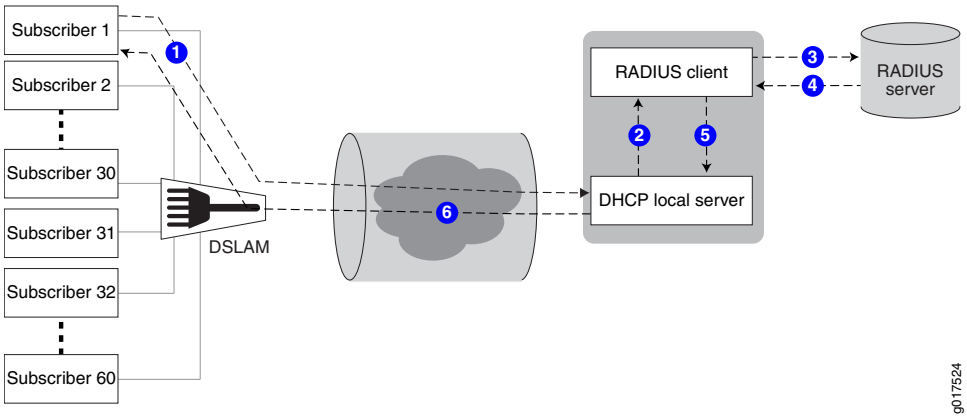
In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router's (switch's) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

Data Flow for RADIUS-Sourced DHCP Options

Figure 1 on page 17 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 1: DHCP Options Data Flow



The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.
2. The DHCP local server initiates authentication with the Junos OS RADIUS client.
3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber's (DHCP client's) client-sourced DHCP options.
4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.
5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.
6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).

7. The subscriber (DHCP client) is configured with the DHCP options.
8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:
   - Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
   - Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
   - Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to by reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

BEST PRACTICE: **For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.**

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

NOTE: **If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the RO flags in the Subscriber Management RADIUS dictionary file. The R value indicates a multivalued reply attribute and the O value indicates an ordered attribute.**

DHCP Options That Cannot Be Centrally Configured

Table 4 on page 19 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 4: Unsupported Opaque DHCP Options

DHCP Option	Option Name	Comments
Option 0	Pad Option	Not supported.
Option 51	IP Address Lease Time	Value is provided by RADIUS attribute 27 (Session-Timeout).
Option 52	Option Overload	Not supported.
Option 53	DHCP Message Type	Value is provided by DHCP local server.
Option 54	Server Identifier	Value is provided by DHCP local server.
Option 55	Parameter Request List	Value is provided by DHCP local server.
Option 255	End	Value is provided by DHCP local server.
–	DHCP magic cookie	Not supported.

Related Documentation

- Monitoring DHCP Options Configured on RADIUS Servers on page 265

RADIUS Accounting Statistics for Subscriber Access Overview

The AAA Service Framework enables you to configure how the router collects and uses accounting statistics for subscriber management.

For example, you can specify when statistics collection is terminated, the order in which different accounting methods are used, the types of statistics collected, and how often statistics are collected. You can also configure the router to request that the RADIUS server immediately update the accounting statistics when certain events occur, such as when a subscriber logs in or when a change of authorization (CoA) occurs.

Subscriber management provides two levels of subscriber accounting—subscriber session and service session. In subscriber session accounting, the router collects statistics for the entire subscriber session. In service session accounting, the router collects statistics for specific service sessions for the subscriber.

NOTE: **Subscriber management counts forwarded packets only. Dropped traffic (for example, as a result of a filter action) and control traffic are not included in the accounting statistics.**

The router uses the RADIUS attributes and Juniper Networks VSAs listed in Table 5 on page 20 to provide the accounting statistics for subscriber and service sessions.

If the session has both IPv4 and IPv6 families enabled, the router reports statistics for both families.

NOTE:

RADIUS reports subscriber statistics as an aggregate of both IPv4 statistics and IPv6 statistics.

- For an IPv4-only configuration, the standard RADIUS attributes report the IPv4 statistics and the IPv6 VSA results are all reported as 0.
- For an IPv6-only configuration, the standard RADIUS attributes and the IPv6 VSA statistics are identical, both reporting the IPv6 statistics.
- When both IPv4 and IPv6 are configured, the standard RADIUS attributes report the combined IPv4 and IPv6 statistics. The IPv6 VSAs report IPv6 statistics.

Table 5: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting

Attribute Number	Attribute Name	Type of Statistics
26–151	IPv6-Acct-Input-Octets	IPv6
26–152	IPv6-Acct-Output-Octets	IPv6
26–153	IPv6-Acct-Input-Packets	IPv6
26–154	IPv6-Acct-Output-Packets	IPv6
26–155	IPv6-Acct-Input-Gigawords	IPv6
26–156	IPv6-Acct-Output-Gigawords	IPv6
47	Acct-Input-Packets	IPv4 and IPv6 aggregation
48	Acct-Output-Packets	IPv4 and IPv6 aggregation
52	Acct-Input-Gigawords	IPv4 and IPv6 aggregation
53	Acct-Output-Gigawords	IPv4 and IPv6 aggregation

Related Documentation

- Configuring Per-Subscriber Session Accounting on page 110
- Configuring Per-Service Session Accounting on page 112
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Understanding RADIUS Accounting Duplicate Reporting

When you configure RADIUS accounting, by default the router sends the accounting reports to the accounting servers in the context in which the subscriber was last authenticated. You can configure RADIUS accounting to send duplicate accounting reports to other servers in the same context or in other contexts.

Layer 3 Wholesale Scenarios

In a Layer 3 wholesale network environment, the wholesaler and retailer might use different RADIUS accounting servers, and both might want to receive accounting reports. In this situation, you can configure RADIUS accounting duplicate reporting, which sends reports to both the wholesaler and the retailer accounting servers. The target to which the duplicate accounting records are sent must be in the default:default logical system:routing instance combination (LS:RI) , also called the *default VRF*.

Table 6 on page 21 shows where subscriber management sends the accounting reports when you enable duplicate reporting. Subscriber management sends duplicate reports based on the access profile in which you configure the **duplication** statement at the **[edit access profile *profile-name* accounting]** hierarchy level, where the subscriber resides, and how the subscriber is authenticated.

NOTE: You can also enable accounting duplicate reporting based on the domain map configuration—you configure subscribers to authenticate with a nondefault routing instance and a target logical system:routing instance of default:default. The accounting reports are then sent to both the authentication context and the default:default context.

Table 6: Duplicate RADIUS Accounting Reporting

Access Profile in Which Duplication Is Configured	Where Subscriber Is Authenticated	Subscriber's Target Logical System/Routing Instance	Accounting Servers Where Accounting Reports Are Sent
retailer A	wholesaler	retailer A	wholesaler and retailer A
retailer A	retailer A	retailer A	wholesaler (default/default context) NOTE: This is the domain map configuration described in the Note preceding this table.
wholesaler	wholesaler and retailer A	retailer A	wholesaler and retailer A

Table 6: Duplicate RADIUS Accounting Reporting *(continued)*

Access Profile in Which Duplication Is Configured	Where Subscriber Is Authenticated	Subscriber's Target Logical System/Routing Instance	Accounting Servers Where Accounting Reports Are Sent
wholesaler and retailer B	wholesaler and retailer A	retailer B	wholesaler, retailer A, and retailer B
not configured (default)	any	any	single report sent to accounting servers in the context in which subscriber was last authenticated

Other Scenarios

For scenarios that are not in a Layer 3 wholesale network environment, you might want to send duplicate accounting records to a different set of RADIUS servers that reside in either the same or a different routing context. Unlike the Layer 3 wholesale scenario, the target for the duplicate RADIUS accounting records does not have to be the default VRF. You can specify a single nondefault VRF—that is, other than the default:default LS:RI combination—as the target. Additionally, you can specify up to five access profiles in the target VRF that list the RADIUS accounting servers that receive the duplicate reports.

For example, you might have a lawful intercept scenario where the subscriber is authenticated in the default domain. An authorized law enforcement organization needs duplicate accounting records for the subscriber to be sent to a mediation device that resides in the organization's networking domain, which lies in a nondefault VRF.

Subscriber management sends duplicate reports to the VRF that you specify with the **vrf-name** statement at the **[edit access profile *profile-name* accounting duplication-vrf]** hierarchy level. Include the **access-profile-name** statement at the same level to designate the access profiles that in turn specify the RADIUS servers that receive the duplicate reports.

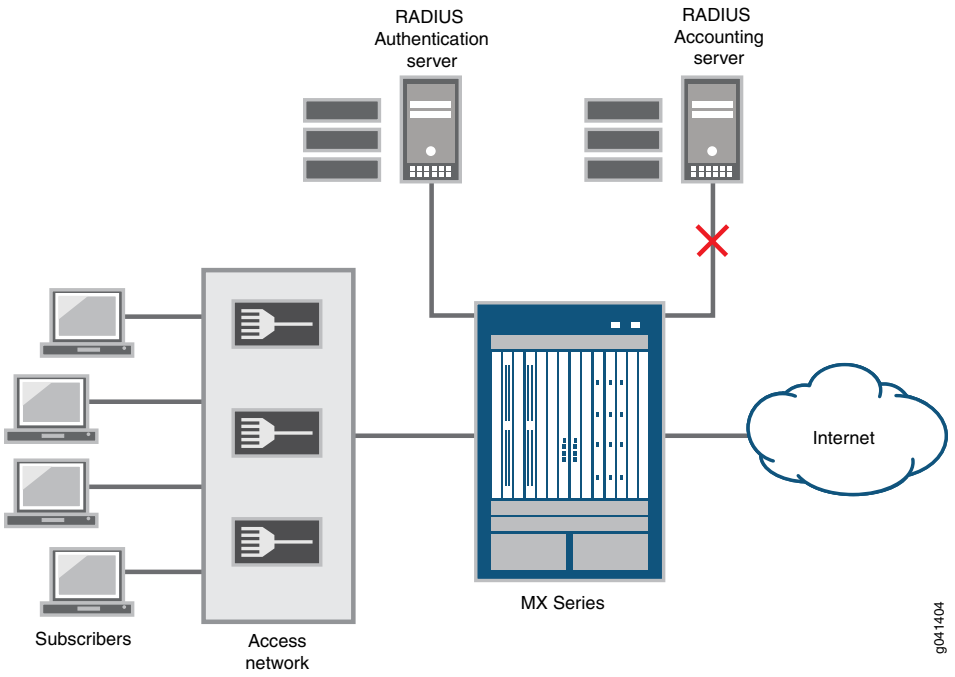
Related Documentation

- Configuring Per-Subscriber Session Accounting on page 110

Preservation of RADIUS Accounting Information During an Accounting Server Outage

If the router loses contact with the RADIUS accounting server, as represented in Figure 2 on page 23, whether due to a server outage or a problem in the network connecting to the server, you can lose all the billing information that would have been received by the server. RADIUS accounting backup preserves the accounting data that accumulates during the outage. If you have not configured RADIUS accounting backup, the accounting data is lost for the duration of the outage from the time when the router has exhausted its attempts to resume contact with the RADIUS server. The configurable retry value determines the number of times the router attempts to contact the server.

Figure 2: Topology with Loss of Access to Accounting Server



By default, the router must wait until the revert timer expires before it can attempt to contact the non-responsive server again. However, when you configure accounting backup, the revert timer is disabled and the router immediately retries its accounting requests as soon as the router fails to receive accounting acknowledgments. Accounting backup follows this sequence:

1. The router fails to receive accounting acknowledgments from the server.
2. The router immediately attempts to contact the accounting server and marks the server as offline if the router does not receive an acknowledgment before exhausting the number of retries.
3. The router next attempts to contact in turn each additional accounting server configured in the RADIUS profile.

   If a server is reached, then the router resumes sending accounting requests to this server.
4. If none of the servers responds or if no other servers are in the profile, the router declares a timeout and begins backing up the accounting data. It withholds all accounting stop messages and does not forward new accounting requests to the server.
5. During the outage, the router sends a single pending accounting stop message to the servers at periodic intervals.
6. If one of the servers acknowledges receipt, then the router sends all the pending stop messages to that server in batches at the same interval until all the stored stop messages have been sent. However, any new accounting requests are sent immediately rather being held and sent periodically.

The router replays accounting stop messages to the server in the correct order because it preserves both the temporal order among subscribers and the causal order between service and session stop requests for each subscriber. Only accounting stop messages are backed up, because they include the start time and duration of sessions and all the accounting statistics. This makes it unnecessary to withhold the accounting start messages, which eventually time out. Interim updates are not backed up and time out as well; if the session remains active, then the next interim update after the server connection is restored provides the interim accounting information.

You can configure the number of accounting stop messages that the router can queue pending restoration of contact with the accounting server. To preserve current accounting data in preference to collecting new accounting data, subscriber logins fail as soon as the maximum number of messages has been withheld. Subscriber logins resume immediately when the pending queue drops below the queue limit.

NOTE: **Service accounting stop messages are withheld for a maximum of ten services per subscriber. If a subscriber attempts to activate an eleventh service while that accounting server is offline, the activation fails.**

The router can hold the pending accounting messages for up to 24 hours. When the configurable maximum holding period passes, all accounting stop messages still in the pending queue are flushed, even if the accounting server has come back online. A consequence of this is that subscriber logins resume immediately if they were failing because the maximum pending limit had been reached.

All pending messages are also flushed in either of the following circumstances:

- If you remove the last accounting server from the access profile, because then there is no place to send the messages.
- If you remove the accounting backup configuration.

While the router is withholding accounting stop messages, you can force the router to attempt contact with the accounting server immediately, rather than allowing it to wait until the periodic interval has expired. When you do so, the router first replays a batch of stop messages to the server, with one of the following outcomes:

- If the router receives an acknowledgment of receipt, then it marks the server as online and begins replaying all remaining pending stop messages in batches.
- If the router does not receive the acknowledgment, then it resumes sending a single pending accounting stop message at the periodic interval.

When a subscriber logs out while the accounting server is offline, the accounting stop requests for the subscriber and the session are queued and replayed to the server when it comes online. In this case, the subscriber session and service session information is retained, so that the router can send a correct accounting request when the server comes back online.

In the event of a graceful Routing Engine switchover while the accounting server is offline, the pending stop messages can be replayed from the active Routing Engine when the server is online again.

NOTE: When RADIUS accounting backup is configured, you must use different servers for RADIUS authentication and accounting. Subscriber authentication fails when the same server is configured for both authentication and accounting.

If the RADIUS server acts on behalf of other back-end RADIUS accounting or authentication servers and forwards requests to them, subscribers can be authenticated but accounting requests are not sent out.

Related Documentation

- Configuring Back-up Options for RADIUS Accounting on page 115
- Forcing the Router to Contact the Accounting Server Immediately on page 116

RADIUS Acct-On and Acct-Off Messages

Subscriber management supports RADIUS Acct-On and Acct-Off messages to indicate the current state of RADIUS accounting support.

RADIUS Acct-On messages indicate that accounting is being supported. Subscriber management issues Acct-On messages in the following situations:

- Accounting is enabled through configuration (for example, an accounting server is configured).
- A new access profile is configured and committed for a logical system/routing instance context. However, no Acct-On message is sent if the accounting server exists prior to the access profile and if it is simply modified.
- The router performs a cold reboot.
- The router performs a warm reboot and there are no subscribers currently logged in.
- The Authd process restarts and there are no active subscribers.

RADIUS Acct-Off messages indicate that accounting in not supported. Subscriber management issues Acct-Off messages in the following situations:

- The Authd process is terminated and there are no active subscribers.
- The router is shut down and accounting servers are currently configured (this action also logs out all current subscribers).
- The router is rebooted and redundancy is disabled.

Related Documentation

- AAA Service Framework Overview on page 3
- Configuring Per-Subscriber Session Accounting on page 110

- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 59

DNS Name Server Address Overview

When a client attempts to access a domain—for example, www.example.com—a request is sent to a Domain Name System (DNS) name server. The name server stores information that correlates domain names with IP addresses; the IP address is used to reach the requested domain. In response to the client request, the name server looks up the IP address for the domain—192.0.43.10 for www.example.com—and returns it to the client.

In your network configuration, you must configure the address of one or more name servers locally on the router or on your RADIUS server. The local configuration supports the following subscriber types:

- DHCPv4 or DHCPv6
- IP over Ethernet (VLAN)
- Terminated PPPoE (IPv4 or IPv6)
- Tunneled PPPoE (IPv4 or IPv6)

You can configure the name server addresses at different levels of granularity: globally (per routing instance), per access profile, or, for DHCP only, per address pool. You can configure more than one name server in a routing instance or access profile by repeating the statement for each address.

Because you can configure name server addresses at more than one level, the address returned to the client is determined by the order of preference among the levels. The preference depends on the client type.

- For DHCP subscribers, the preference in descending order is

  RADIUS > DHCP address pool > access profile > global

- For non-DHCP subscribers, the preference in descending order is

  RADIUS > access profile > global

According to the preference order, a name server address configured in RADIUS is preferred by all subscriber types over all other configuration levels. For all subscriber types, the global name server address is used only when no other name server addresses are configured. When a name server address is configured only in a DHCP address pool, then no address is available to non-DHCP subscribers.

When you configure multiple addresses for a name server, the order in which you configure them determines the preference within that configuration. The preference according to configuration level supersedes this ordering.

For IPv4 name server addresses, you can use either of two statements to configure the address. Addresses configured with the domain-name-server-inet statement take precedence over addresses configured with the domain-name-server statement.

There is no restriction on the number of DNS name server addresses that you can configure. For DHCP subscribers, all the addresses are sent in DHCP messages. However, only two addresses—determined by preference order—are sent to PPP subscribers.

All changes in these locally configured DNS name servers affect only new subscribers that subsequently log in. Existing subscribers are not affected by the changes.

Related Documentation

- Configuring DNS Name Server Addresses for Subscriber Management on page 150
- *DHCP Attributes for Address-Assignment Pools*
- *Configuring DHCP Client-Specific Attributes*

Understanding Session Options for Subscriber Access

You can limit subscriber access by configuring a session timeout or an idle timeout. Use a session timeout to specify a fixed period of time that the subscriber is permitted to have access. Use an idle timeout to specify a maximum period of time that the subscriber can be idle. You can use these timeouts separately or together. By default, neither timeout is present.

NOTE: **For all subscriber types other than DHCP (such as L2TP-tunneled and PPP-terminated subscribers), the session timeout value limits the subscriber session. For DHCP subscribers, the session timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.**

The idle timeout is based on accounting statistics for the subscriber. The router determines subscriber inactivity by monitoring data traffic, both upstream from the user and downstream to the user. Control traffic is ignored. The subscriber is not considered idle as long as data traffic is detected in either direction.

When either timeout period expires, the non-DHCP subscribers are gracefully logged out, similarly to a RADIUS-initiated disconnect or a CLI-initiated logout. DHCP subscribers are disconnected. The Acct-Terminate-Cause [RADIUS attribute 49] value includes a reason code of 5 for a session timeout and a code of 4 for an idle timeout.

You can configure these limitations to subscriber access on a per-subscriber basis by using the RADIUS attributes Session-Timeout [27] and Idle-Timeout [28]. RADIUS returns these attributes in Access-Accept messages in response to Access-Request messages from the access server.

Service providers often choose to apply the same limitations to large numbers of subscribers. You can reduce the RADIUS provisioning effort for this scenario by defining the limitations for subscribers in an access profile on a per-routing-instance basis. If you do so, RADIUS attributes subsequently returned for a particular subscriber logged in with the profile override the per-routing-instance values.

The available range for setting a timeout is the same whether you configure it in the CLI or through the RADIUS attributes. Session timeouts can be set for 1 minute through 527,040 minutes in the CLI and the corresponding number of seconds (60 through 31,622,400) in the Session-Timeout attribute [27]. Idle timeouts can be set for 10 minutes through 1440 minutes in the CLI and the corresponding number of seconds (600 through 86,400) in the Idle-Timeout attribute [28].

The router interprets the values in the attributes to conform to the supported ranges. For example, for Session-Timeout [27]:

- A value of zero is treated as no timeout.
- A value in the range 1 through 59 is raised to 60 seconds.
- A value that exceeds 31,622,400 is reduced to 31,622,400 seconds.

For Idle-Timeout [28]:

- A value of zero is treated as no timeout.
- A value in the range 1 through 599 is raised to 600 seconds.
- A value that exceeds 86,400 is reduced to 86,400 seconds.

In configurations using dynamically created subscriber VLANs, the idle timeout also deletes the inactive subscriber VLANs when the inactivity threshold has been reached. In addition to deleting inactive dynamic subscriber VLANs, the idle timeout also removes dynamic VLANs when no client sessions were ever created (for example, in the event no client sessions are created on the dynamic VLAN or following the occurrence of an error during session creation or client authentication where no client sessions are created on the dynamic VLAN).

When using the idle timeout for dynamic VLAN removal, keep the following in mind:

- The idle timeout period begins after a dynamic subscriber VLAN interface is created or traffic activity stops on a dynamic subscriber VLAN interface.
- If a new client session is created or a client session is reactivated successfully, the client idle timeout resets.
- The removal of inactive subscriber VLANs functions only with VLANs that have been authenticated.

Related Documentation

- RADIUS IETF Attributes Supported by the AAA Service Framework on page 37
- Configuring Subscriber Session Options on page 152
- Removing Inactive Dynamic Subscriber VLANs on page 29

Removing Inactive Dynamic Subscriber VLANs

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both. In configurations using dynamically created subscriber VLANS, the idle timeout also:

- Deletes the inactive subscriber VLANs when the inactivity threshold has been reached.
- Removes dynamic VLANs when no client sessions were ever created (for example, in the event no client sessions are created on the dynamic VLAN or following the occurrence of an error during session creation or client authentication where no client sessions are created on the dynamic VLAN).

NOTE: **To configure the idle timeout attribute in RADIUS, refer to the documentation for your RADIUS server.**

To remove inactive dynamic subscriber VLANS:

1. Edit session options for the router access profile.

   ```
   [edit]
   user@host# edit access profile profile-name session-options
   ```

2. Configure the maximum period a subscriber session can remain idle.

   ```
   [edit access profile profile-name session-options]
   user@host# set client-idle-timeout minutes
   ```

Related Documentation

- Understanding Session Options for Subscriber Access on page 27
- Configuring Subscriber Session Options on page 152
- client-idle-timeout on page 197

AAA Configuration Testing and Troubleshooting

Subscriber management supports a test feature that enables you to check the AAA configuration of a subscriber. You might use the test feature to verify the subscriber's AAA settings and to help troubleshoot or isolate subscriber login problems. The AAA test process creates a pseudo session that authenticates the subscriber, allocates an address for the subscriber, and issues an accounting start packet. The process then issues an accounting stop request, releases the address, and terminates the pseudo session.

The AAA test results provide details about the attributes that subscriber management assigns to the subscriber during login. The attributes might be assigned by RADIUS, a dynamic profile, static interface configuration, or might be statically assigned. You can test the AAA configuration for DHCP, PPP, and authd-lite subscribers. For L2TP clients, the AAA test process displays all tunnel parameters but does not create an actual tunnel session.

NOTE: The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

Related Documentation

- Testing a Subscriber AAA Configuration on page 268

CHAPTER 2

Dynamic Service Activation

Using RADIUS Dynamic Requests for Subscriber Access Management

RADIUS dynamic requests provide an efficient way to centrally manage subscriber sessions. The AAA Service Framework's RADIUS dynamic request support allows RADIUS servers to initiate user-related operations, such as a termination operation, by sending unsolicited request messages to the router. Without the RADIUS dynamic request feature, the only way to disconnect a RADIUS user is from the router, which can be cumbersome and time-consuming in large networks.

In a typical client-server RADIUS environment, the router functions as the client and initiates requests sent to the remote RADIUS server. However, when using RADIUS dynamic requests, the roles are reversed. For example, during a disconnect operation, the remote RADIUS server performs as the client and initiates the request (the disconnect action) — the router functions as the server in the relationship.

You create an access profile to configure the router to support RADIUS dynamic requests. This configuration enables the router to receive and act on the following types of messages from remote RADIUS servers:

- Access-Accept messages—Dynamically activate services based on attributes in RADIUS Access-Accept messages received when a subscriber logs in.
- Change-of-Authorization (CoA) messages—Dynamically modify active sessions based on attributes in CoA messages. CoA messages can include service creation requests, deletion requests, RADIUS attributes, and Juniper Networks VSAs.
- Disconnect messages—Immediately terminate specific subscriber sessions.

Related Documentation

- Dynamic Service Activation During Login Overview on page 32
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 32
- RADIUS-Initiated Disconnect Overview on page 34

- Configuring RADIUS-Initiated Dynamic Request Support on page 148
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 5
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 72

Dynamic Service Activation During Login Overview

The AAA Service Framework enables the router to dynamically activate subscriber services as part of a subscriber login operation.

The framework sets up the subscriber session and then completes the service action specified by the Juniper Networks VSA 26–65 that is received in the Access-Accept message. If the service request is unsuccessful, the framework logs out the subscriber.

Related Documentation

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 31
- Configuring RADIUS-Initiated Dynamic Request Support on page 148
- RADIUS-Initiated Disconnect Overview on page 34

RADIUS-Initiated Change of Authorization (CoA) Overview

The AAA Service Framework uses CoA messages to dynamically modify active subscriber sessions. For example, RADIUS attributes in CoA messages might instruct the framework to create, modify, or terminate a subscriber service.

CoA Messages

Dynamic request support enables the router to receive and process unsolicited CoA messages from external RADIUS servers. RADIUS-initiated CoA messages use the following codes in request and response messages:

- CoA-Request (43)
- CoA-ACK (44)
- CoA-NAK (45)

Qualifications for Change of Authorization

To complete the change of authorization for a user, you specify identification attributes and session attributes. The identification attributes identify the subscriber. Session attributes specify the operation (activation or deactivation) to perform on the subscriber's session and also include any client attributes for the session (for example, QoS attributes). The AAA Service Framework handles the actual request.

Table 7 on page 33 shows the identification attributes for CoA operations.

NOTE: Using the Acct-Session-ID attribute to identify the subscriber session is more explicit than using the User-Name attribute. When you use the Acct-Session-ID, the attribute identifies the specific subscriber and session. When you use the User-Name as the identifier, the CoA operation is applied to the first session that was logged in with the specified username. However, because a subscriber might have multiple sessions associated with the same username, the first session might not be the correct session for the CoA operation.

Table 7: Identification Attributes

Attribute	Description
User-Name [RADIUS attribute 1]	Subscriber username.
Acct-Session-ID [RADIUS attribute 44]	Specific subscriber and session.

Table 8 on page 33 shows the session attributes for CoA operations. Any additional client attributes that you include depend on your particular session requirements.

Table 8: Session Attributes

Attribute	Description
Activate-Service [Juniper Networks VSA 26–65]	Service to activate for the subscriber.
Deactivate-Service [Juniper Networks VSA 26–66]	Service to deactivate for the subscriber.

Message Exchange

The RADIUS server and the AAA Service Framework on the router exchange messages using UDP. The CoA-Request message sent by the RADIUS server has the same format as the Disconnect-Request packet that is sent for a disconnect operation.

The response is either a CoA-ACK or a CoA-NAK message:

- If the AAA Service Framework successfully changes the authorization, the response is a RADIUS-formatted packet with a CoA-ACK message, and the data filter is applied to the session.
- If AAA Service Framework is unsuccessful, the request is malformed, or attributes are missing, the response is a RADIUS-formatted packet with a CoA-NAK message.

NOTE: The AAA Service Framework processes one dynamic request at a time per subscriber. If the framework receives a second dynamic request (either another CoA or a Disconnect-Request) while processing a previous request for the same subscriber, the framework responds with a CoA-NAK message.

Related Documentation

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 31
- Dynamic Service Activation During Login Overview on page 32
- RADIUS-Initiated Disconnect Overview on page 34
- Configuring RADIUS-Initiated Dynamic Request Support on page 148

RADIUS-Initiated Disconnect Overview

This section describes the AAA Service Framework's support for RADIUS-initiated disconnect dynamic requests. The AAA Service Framework uses disconnect messages to dynamically terminate active subscriber sessions.

Disconnect Messages

To centrally control the disconnection of remote access subscribers, the RADIUS dynamic request feature on the router receives and processes unsolicited messages from RADIUS servers.

The dynamic request feature uses the existing format of RADIUS disconnect request and response messages. RADIUS-initiated disconnect uses the following codes in its RADIUS request and response messages:

- Disconnect-Request (40)
- Disconnect-ACK (41)
- Disconnect-NAK (42)

Qualifications for Disconnect

For the AAA Service Framework to disconnect a user, the Disconnect-Request message must contain an attribute with an accounting session ID. The Disconnect-Request message can contain an Acct-Session-Id (44) attribute or an Acct-Multi-Session-Id (50) attribute for the session ID or both. If both the Acct-Session-Id and Acct-Multi-Session-Id attributes are present in the request, the router uses both attributes. If the User-Name (1) attribute is also present in the request, the username and accounting session ID are used to perform the disconnection. The AAA Service Framework handles the actual request.

Message Exchange

The RADIUS server and the AAA Service Framework exchange messages using UDP. The Disconnect-Request message sent by the RADIUS server has the same format as the CoA-Request packet that is sent for a change of authorization operation.

The disconnect response is either a Disconnect-ACK or a Disconnect-NAK message:

- If the AAA Service Framework successfully disconnects the user, the response is a RADIUS-formatted packet with a Disconnect-ACK message.

- If the AAA Service Framework cannot disconnect the user, the request is malformed, or attributes are missing from the request, the response is a RADIUS-formatted packet with a Disconnect-NAK message.

NOTE: The AAA Service Framework processes one dynamic request at a time per subscriber. If the framework receives a second dynamic request while processing a previous request (either a CoA or another Disconnect-Request) for the same subscriber, the framework responds with a Disconnect-NAK message.

Related Documentation

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 31
- Dynamic Service Activation During Login Overview on page 32
- Configuring RADIUS-Initiated Dynamic Request Support on page 148

CHAPTER 3

RADIUS Attributes and VSA Tables

RADIUS IETF Attributes Supported by the AAA Service Framework

Table 9 on page 38 describes the RADIUS IETF attributes that the Junos OS AAA Service Framework supports.

NOTE: A "Yes" entry in the Dynamic CoA Support column indicates that the attribute can be dynamically configured by Access-Accept messages and dynamically modified by CoA-Request messages.

Table 9: Supported RADIUS IETF Attributes

Attribute Number	Attribute Name	Description	Dynamic CoA Support
1	User-Name	• Name of user to be authenticated. • Configurable username override.	No
2	User-Password	• Password of user to be authenticated by Password Authentication Protocol (PAP). • Configurable password override.	No
4	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user.	No
5	NAS-Port	Physical port number of the NAS that is authenticating the user. For a tunneled PPP user in an L2TP LNS session, there is no physical port. In this case, the port value is reported as 4194303.	No
6	Service-Type	Type of service the user has requested or the type of service to be provided.	No
8	Framed-IP-Address	• IP address to be configured for the user. • 0.0.0.0 or absence is interpreted as 255.255.255.254.	No
9	Framed-IP-Netmask	• IP network to be configured for the user when the user is a router or switch to a network. • Absence implies 255.255.255.255.	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
11	Filter-Id	Name of a subscriber firewall filter, formatted as follows: • For an IPv4 input filter—IPv4-ingress:*ingress-filter-name* • For an IPv4 output filter—IPv4-egress:*egress-filter-name* • For an IPv6 input filter—IPv6-ingress:*ingress-filter-name* • For an IPv6 output filter—IPv6-egress:*egress-filter-name* RADIUS accounting request messages, Acct-Start and Acct-Stop, can include more than one Filter-Id attribute, one of each of the listed types. However, RADIUS Access-Accept messages can include only one attribute instance. The value is always treated as an IPv4 input filter name.	Yes
18	Reply-Message	• Text that may be displayed to the user. • Only the first instance of this attribute is used.	No
22	Framed-Route	String that provides routing information to be configured for the user on the NAS in the format: **<addr>[/<maskLen>] [<nexthop> [<cost>]] [tag <tagValue>] [distance <distValue>]**	Yes
25	Class	Arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server.	No
27	Session-Timeout	Maximum number of consecutive seconds of service to be provided to the user before termination of the session.	No
31	Calling-Station-ID	Phone number from which the call originated.	No
32	NAS-Identifier	NAS originating the request.	No
40	Acct-Status-Type	Whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update).	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.	No
42	Acct-Input-Octets	Number of octets that have been received from the port during the time this service has been provided.	No
43	Acct-Output-Octets	Number of octets that have been sent to the port during the time this service has been provided.	No
44	Acct-Session-ID	Unique accounting identifier that makes it easy to match start and stop records in a log file. The identifier can be in one of the following formats: • **decimal**—For example, **435264** • **description**—In the generic format, **jnpr** *interface-specifier:subscriber-session-id*; For example, **jnpr fastEthernet 3/2.6:1010101010101**	No
45	Acct-Authentic	Method by which user was authentication: whether by RADIUS, the NAS itself, or another remote authentication protocol.	No
46	Acct-Session-Time	Number of seconds that the user has received service	No
47	Acct-Input-Packets	Number of packets that have been received from the port during the time this service has been provided to a framed user.	No
48	Acct-Output-Packets	Number of packets that have been sent to the port in the course of delivering this service to a framed user.	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
49	Acct-Terminate-Cause	Reason the service (a PPP session) was terminated. The service can be terminated for the following reasons: • User Request (1)—User initiated the disconnect (log out). • Idle Timeout (4)—Idle timer has expired. • Session Timeout (5)—Client reached the maximum continuous time allowed on the service or session. • Admin Reset (6)—System administrator terminated the session. • Port Error (8)—PVC failed; no hardware or no interface. • NAS Error (9)—Negotiation failures, connection failures, or address lease expiration. • NAS Request (10)—PPP challenge timeout, PPP request timeout, tunnel establishment failure, PPP bundle failure, IP address lease expiration, PPP keep-alive failure, tunnel disconnect, or an unaccounted-for error.	No
52	Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^{32} during the time this service has been provided. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update.	No
53	Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^{32} in the course of delivering this service. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update.	No
55	Event-Timestamp	Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	No
61	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user. For a tunneled PPP user in an L2TP LNS session, there is no physical port. In this case, the port type is **Virtual**.	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
64	Tunnel-Type	• Tunneling protocol to use (in the case of a tunnel initiator) or the tunneling protocol already in use (in the case of a tunnel terminator). • Only L2TP tunnels are currently supported.	No
65	Tunnel-Medium-Type	• Transport medium to use when creating a tunnel for protocols that can operate over multiple transports. • Only IPv4 is currently supported.	No
66	Tunnel-Client-Endpoint	Address of the initiator end of the tunnel (LAC).	No
67	Tunnel-Server-Endpoint	Address of the server end of the tunnel (LNS).	No
69	Tunnel-Password	Encrypted password used to authenticate to a remote server. Recommended over using VSA Tunnel-Password [26-9] because of the encryption. Do not use both this attribute and the VSA.	No
82	Tunnel-Assignment -Id	Tunnel to which a session is assigned. When user profiles share the same values for Tunnel-Assignment-Id, Tunnel-Server-Endpoint, and Tunnel-Type, the LAC can group these users into the same tunnel. This grouping enables fewer tunnels to be created. (LAC)	No
83	Tunnel-Preference	• Included in each set of tunneling attributes to indicate the relative preference assigned to each tunnel when more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator. • Included in the Tunnel-Link-Start, the Tunnel-Link-Reject, and the Tunnel-Link-Stop packets (LAC only).	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
85	Acct-Interim-Interval	Number of seconds between each interim accounting update for this session. The router uses the following guidelines for interim accounting: • Attribute value is within the acceptable range (from 600 through 86,400 seconds)—Accounting is updated at the specified interval. • Attribute value of 0—No RADIUS accounting is performed. • Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds). • Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds). NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).	No
87	NAS-Port-Id	Text string that identifies the physical interface of the NAS that is authenticating the user. For a tunneled PPP user in an L2TP LNS session, there is no physical port, and the NAS-Port-Id value has the following format: *media:local address:peer address: local tunnel id:peer tunnel id: local session id:peer session id: call serial number*. For example, lp:172.20.0.1:192.168.0.2: 3341:21031:16138:11846:2431. The local information refers to the LNS and the peer information refers to the LAC.	No
88	Framed-Pool	Name of an assigned address pool to use to assign an address for the user.	No
90	Tunnel-Client-Auth-Id	Name of the tunnel initiator (LAC) used during the authentication phase of tunnel establishment.	No

Table 9: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description	Dynamic CoA Support
91	Tunnel-Server-Auth-Id	Name of the tunnel terminator (LNS) used during the authentication phase of tunnel establishment.	No
95	NAS-IPv6-Address	Address of the NAS that is requesting authentication of the user.	No
96	Framed-Interface-ID	Interface identifier that is configured for the user.	No
97	Framed-IPv6-Prefix	IPv6 prefix and address that are configured for the user. Prefix lengths of 128 are associated with host addresses. Prefix lengths less than 128 are associated with NDRA prefixes.	No
98	Login-IPv6-Host	System the user connects to when the Login-Service attribute is included.	No
99	Framed-IPv6-Route	IPv6 routing information that is configured for the user.	Yes
100	Framed-IPv6-Pool	Name of the assigned pool used to assign the address and IPv6 prefix for the user.	No
123	Delegated-IPv6-Prefix	IPv6 prefix that is delegated to the user.	No
242	Ascend-Data-Filter	Binary data that specifies RADIUS policy definitions.	Yes

Related Documentation

- AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 54
- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 59

Juniper Networks VSAs Supported by the AAA Service Framework

Table 10 on page 45 describes Juniper Networks VSAs supported by the Junos OS AAA Service Framework. The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).

NOTE: A "Yes" entry in the Dynamic CoA Support column indicates that the attribute can be dynamically configured by Access-Accept messages and dynamically modified by CoA-Request messages.

Table 10: Supported Juniper Networks VSAs

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-1	Virtual-Router	Client logical system:routing instance name. Allowed only from AAA server for "default" logical system:routing instance. When this VSA is not included in the subscriber profile, the routing instance assigned to the subscriber—the one in which the subscriber session comes up—varies by subscriber type. For DHCP and PPPoE subscribers, it is the default routing instance. For L2TP tunnel subscribers, it is the routing instance in which the tunnel resides, whether default or non-default. If the tunnel routing instance is not default and you want the L2TP session to be in the default routing instance, you must use the Virtual-Router VSA to set the desired routing instance.	string: *logical system:routing instance*	No
26-4	Primary-DNS	Client DNS address negotiated during IPCP.	integer: 4-byte *primary-dns-address*	No
26-5	Secondary-DNS	Client DNS address negotiated during IPCP	integer: 4-byte *secondary-dns-address*	No
26-6	Primary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte *primary-wins-address*	No
26-7	Secondary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte *secondary-wins-address*	No
26-8	Tunnel-Virtual-Router	Virtual router name for tunnel connection.	string: *tunnel-virtual-router*	No
26-9	Tunnel-Password	Tunnel password in cleartext. Do not use both this VSA and the standard RADIUS attribute Tunnel-Password [69]. The standard attribute is recommended because the password is encrypted when that attribute is used.	string: *tunnel-password*	No
26-10	Ingress-Policy-Name	Input policy name to apply to client interface.	string: *input-policy-name*	Yes

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-11	Egress-Policy-Name	Output policy name to apply to client interface.	string: *output-policy-name*	Yes
26-23	IGMP-Enable	Whether IGMP is enabled or disabled on a client interface.	integer: • 0=disable • 1=enable	Yes
26-25	Redirect-VRouter-Name	Client logical system:routing instance name indicating to which logical system:routing instance the request is redirected for user authentication.	string: *logical-system:routing-instance*	No
26–30	Tunnel-Nas-Port-Method	Method that determines whether the RADIUS server conveys to the LNS the physical NAS port number identifier and the type of the physical port, such as Ethernet or ATM. This information is conveyed only when the VSA value is 1. The VSA is formatted such that the first octet indicates the tunnel and the remaining three bytes are the attribute value.	4-octet integer: • 0 = none • 1 = Cisco CLID	Yes
26-31	Service-Bundle	The SSC service bundle.	string *bundle-name*	No
26-33	Tunnel-Max-Sessions	Maximum number of sessions allowed in a tunnel.	integer: 4-octet	No
26-34	Framed-IP-Route-Tag	Route tag to apply to returned framed-ip-address.	integer: 4-octet	No
26-42	Input-Gigapackets	Number of times the input-packets attribute rolls over its 4-octet field.	Integer	No
26-43	Output-Gigapackets	Number of times the output-packets attribute rolls over its 4-octet field.	Integer	No
26-47	Ipv6-Primary-DNS	Client primary IPv6 DNS address negotiated by DHCP.	hexadecimal string: *ipv6-primary-dns-address*	No
26-48	Ipv6-Secondary-DNS	Client secondary IPv6 DNS address negotiated by DHCP.	hexadecimal string: *ipv6-secondary-dns-address*	No

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-51	Tunnel-Disconnect-Cause-Info	Disconnect cause when a tunneled subscriber is disconnected, and the termination is initiated by the L2TP layer of the LNS. The PPP Disconnect Cause Code (L2TP AVP 46) is included in VSA 26-51 in the Accounting-Stop message that the router sends to the RADIUS server.	hexadecimal string: *tunnel-disconnect-cause-info*	No
26-55	DHCP-Options	Client DHCP options.	string: *dhcp-options*	No
26-56	DHCP-MAC-Address	Client MAC address.	string: *mac-address*	No
26-57	DHCP-GI-Address	DHCP relay agent IP address.	integer: 4-octet	No
26-58	LI-Action	Traffic mirroring action. For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26–59. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs. If the CoA action is to stop mirroring (VSA 26–58 value is 0), then the values of the other three attributes in the CoA message must match the existing attribute values, or the action fails.	Salt-encrypted integer 0=stop mirroring 1=start mirroring 2=no action	Yes
26-59	Med-Dev-Handle	Identifier that associates mirrored traffic to a specific subscriber. For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26–59. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs.	Salt-encrypted string	No

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-60	Med-Ip-Address	IP address of content destination device to which mirrored traffic is forwarded. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs.	Salt-encrypted IP address	No
26-61	Med-Port-Number	UDP port in the content destination device to which mirrored traffic is forwarded. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs.	Salt-encrypted integer	No
26-63	Interface-Desc	Text string that identifies the subscriber's access interface.	string: *interface-description*	No
26-64	Tunnel-Group	Name of the tunnel group (profile) assigned to a domain map.	string: *tunnel-group-name*	No
26-65	Activate-Service	Service to activate for the subscriber. Tagged VSA, which supports 8 tags (1-8).	string: *service-name*	Yes
26-66	Deactivate-Service	Service to deactivate for the subscriber.	string: *service-name*	No
26-69	Service-Statistics	Whether statistics for the service is enabled or disabled. Tagged VSA, which supports 8 tags (1-8).	• 0 = disable • 1 = enable time statistics • 2 = enable time and volume statistics	Yes
26-70	Ignore-DF-Bit	State of the Ignore Don't Fragment (DF) bit on client interface	integer: • 0 = do not ignore • 1 = ignore	No
26-71	IGMP-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes
26-72	IGMP-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-74	MLD-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes
26-75	MLD-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes
26-77	MLD-Version	MLD protocol version.	integer: 1-octet • 1=MLD version 1 • 2=MLD version 2	Yes
26-78	IGMP-Version	IGMP protocol version.	integer: 1-octet • 1=IGMP version 1 • 2=IGMP version 2 • 3=IGMP version 3	Yes
26-83	Service-Session	Name of the service.	string: *service-name*	No
26–84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile IP registration.	integer: 4-octet	No
26–85	Mobile-IP-SPI	Security parameter index number for Mobile IP registration.	integer: 4-octet	No
26–86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration.	string: key	No
26–87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration.	integer: 4-octet	No
26–89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration.	integer: 4-octet	No
26–91	Tunnel-Switch-Profile	Tunnel switch profile that determines whether a subscriber session is switched to a second session to a remote LNS. Takes precedence over tunnel switch profiles applied in any other manner,	string: *profile-name*	No
26–92	L2C-Up-Stream-Data	Actual upstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration.	string: actual upstream rate access loop parameter (ASCII encoded)	

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26–93	L2C-Down-Stream-Data	Actual downstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration.	string: actual downstream rate access loop parameter (ASCII encoded)	
26-97	IGMP-Immediate-Leave	IGMP Immediate Leave.	integer: 4-octet • 0=disable • 1=enable	Yes
26-100	MLD-Immediate-Leave	MLD Immediate Leave.	integer: 4-octet • 0=disable • 1=enable	Yes
26-106	IPv6-Ingress-Policy-Name	Input policy name to apply to a user IPv6 interface.	string: *policy-name*	Yes
26-107	IPv6-Egress-Policy-Name	Output policy name to apply to a user IPv6 interface.	string: *policy-name*	Yes
26-108	CoS-Traffic-Control-Profile-Parameter-Type	CoS traffic-shaping parameter type and description: • **T01**: Scheduler-map name • **T02**: Shaping rate • **T03**: Guaranteed rate • **T04**: Delay-buffer rate • **T05**: Excess rate • **T06**Traffic-control profile • **T07**: Shaping mode • **T08**: Byte adjust • **T09**: Adjust minimum • **T10**: Excess-rate high • **T11**: Excess-rate low • **T12**: Shaping rate burst • **T13**: Guaranteed rate burst	Two parts, delimited by white space: • Parameter type • Parameter value Examples: • **T01 smap_basic** • **T02 50m** • **T03 1m** • **T04 2000** • **T05 200** • **T06 tcp-gold** • **T07 frame-mode** • **T08 50**	Yes
26-109	DHCP-Guided-Relay-Server	IP address of DHCP server that DHCP relay agent uses to forward the discover PDUs.	integer: 4-byte *ip-address*	No
26–110	Acc-Loop-Cir-Id	Identification of the subscriber node connection to the access node.	string: up to 63 ASCII characters	
26–111	Acc-Aggr-Cir-Id-Bin	Unique identification of the DSL line.	integer: 8-octet	

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26–112	Acc-Aggr-Cir-Id-Asc	Identification of the uplink on the access node, as in the following examples: • Ethernet access aggregation—**ethernet** ***slot/port [:inner-vlan-id] [:outer-vlan-id]*** • ATM aggregation—**atm** ***slot/port:vpi.vci***	string: up to 63 ASCII characters	
26–113	Act-Data-Rate-Up	Actual upstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	
26–114	Act-Data-Rate-Dn	Actual downstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	
26–115	Min-Data-Rate-Up	Minimum upstream data rate configured for the subscriber.	integer: 4-octet	
26–116	Min-Data-Rate-Dn	Minimum downstream data rate configured for the subscriber.	integer: 4-octet	
26–117	Att-Data-Rate-Up	Maximum upstream data rate that the subscriber can attain.	integer: 4-octet	
26–118	Att-Data-Rate-Dn	Maximum downstream data rate that the subscriber can attain.	integer: 4-octet	
26–119	Max-Data-Rate-Up	Maximum upstream data rate configured for the subscriber.	integer: 4-octet	
26–120	Max-Data-Rate-Dn	Maximum downstream data rate configured for the subscriber.	integer: 4-octet	
26–121	Min-LP-Data-Rate-Up	Minimum upstream data rate in low power state configured for the subscriber.	integer: 4-octet	
26–122	Min-LP-Data-Rate-Dn	Minimum downstream data rate in low power state configured for the subscriber.	integer: 4-octet	
26–123	Max-Interlv-Delay-Up	Maximum one-way upstream interleaving delay configured for the subscriber.	integer: 4-octet	
26–124	Act-Interlv-Delay-Up	Subscriber's actual one-way upstream interleaving delay..	integer: 4-octet	

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26–125	Max-Interlv-Delay-Dn	Maximum one-way downstream interleaving delay configured for the subscriber.	integer: 4-octet	
26–126	Act-Interlv-Delay-Dn	Subscriber's actual one-way downstream interleaving delay.	integer: 4-octet	
26–127	DSL-Line-State	State of the DSL line.	integer: 4-octet • 1 = Show uptime • 2 = Idle • 3 = Silent	
26–128	DSL-Type	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated.		
26-130	Qos-Set-Name	Interface set to apply to the dynamic profile.	string: *interface-set-name*	No
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service. Tagged VSA, which supports 8 tags (1-8).	• range = 600 through 86400 seconds • 0 = disabled NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).	Yes
26–141	Downstream-Calculated-QoS-Rate	Calculated (adjusted) downstream QoS rate in Kbps as set by the ANCP configuration.	range = 1000 through 4,294,967,295	
26–142	Upstream-Calculated-QoS-Rate	Calculated (adjusted) upstream QoS rate in Kbps as set by the ANCP configuration.	range = 1000 through 4,294,967,295	
26-143	Max-Clients-Per-Interface	Maximum allowable client sessions per interface. For DHCP clients, this value is the maximum sessions per logical interface. For PPPoE clients, this value is the maximum sessions (PPPoE interfaces) per PPPoE underlying interface.	integer: 4-octet	No

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-146	CoS-Scheduler-Pmt-Type	CoS scheduler parameter type and description: • Null: CoS scheduler name • **T01**: CoS scheduler transmit rate • **T02**: CoS scheduler buffer size • **T03**: CoS scheduler priority • **T04**: CoS scheduler drop-profile low • **T05**: CoS scheduler drop-profile medium-low • **T06**: CoS scheduler drop-profile medium-high • **T07**: CoS scheduler drop-profile high • **T08**: CoS scheduler drop-profile any	Three parts, delimited by white space: • Scheduler name • Parameter type • Parameter value Examples: • **be_sched** • **be_sched T01 12m** • **be_sched T02 26**	Yes
26-151	IPv6-Acct-Input-Octets	IPv6 receive octets.	integer	No
26-152	IPv6-Acct-Output-Octets	IPv6 transmit octets.	integer	No
26-153	IPv6-Acct-Input-Packets	IPv6 receive packets.	integer	No
26-154	IPv6-Acct-Output-Packets	IPv6 transmit packets.	integer	No
26-155	IPv6-Acct-Input-Gigawords	IPv6 receive gigawords.	integer	No
26-156	IPv6-Acct-Output-Gigawords	IPv6 transmit gigawords.	integer	No
26-158	PPPoE-Padn	Route add for PPPoE sessions	string	No
26-161	IPv6-Delegated-Pool-Name	Address pool used to locally allocate a delegated prefix (IA_PD).	string	No
26-162	Tx-Connect-Speed	Indication of user's connection.	string	No
26-163	Rx-Connect-Speed	Indication of user's connection.	string	No
26-173	Service-Activate-Type	Indication of service activation type. This is a tagged attribute.	integer: 4-octet • 1 = dynamic-profile • 2 = op-script	No
26-174	Client-Profile-Name	Enables the RADIUS server to override the client dynamic profile in the Access-Accept message.	string	No

Table 10: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26–177	Cos-Shaping-Rate	Effective downstream shaping rate for subscriber.	string	No

Related Documentation

- AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 54
- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 59

AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS

Table 11 on page 54 shows the RADIUS attributes and Juniper Networks VSAs support in AAA access messages. A checkmark in a column indicates that the message type supports that attribute.

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
1	User-Name	✓	✓	–	–	✓	✓
2	User-Password	✓	–	–	–	–	–
3	CHAP-Password	✓	–	–	–	–	–
4	NAS-IP-Address	✓	–	–	–	–	–
5	NAS-Port	✓	–	–	–	–	–
6	Service-Type	✓	✓	–	–	–	–
7	Framed-Protocol	✓	✓	–	–	–	–
8	Framed-IP-Address	✓	✓	–	–	✓	–
9	Framed-IP-Netmask	–	✓	–	–	–	–
11	Filter-Id	–	✓	–	–	–	–
12	Framed-MTU	✓	–	–	–	–	–
18	Reply-Message	–	✓	✓	✓	–	–

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
22	Framed-Route	–	✓	–	–	–	–
25	Class	–	✓	–	–	–	–
26-1	Virtual-Router	–	✓	–	–	✓	–
26-4	Primary-DNS	–	✓	–	–	–	–
26-5	Secondary-DNS	–	✓	–	–	–	–
26-6	Primary-WINS	–	✓	–	–	–	–
26-7	Secondary-WINS	–	✓	–	–	–	–
26-8	Tunnel-Virtual-Router	–	✓	–	–	–	–
26-9	Tunnel-Password	–	✓	–	–	–	–
26-10	Ingress-Policy-Name	–	✓	–	–	–	–
26-11	Egress-Policy-Name	–	✓	–	–	–	–
26-23	IGMP-Enable	–	✓	–	–	–	–
26-25	Redirect-VR-Name	–	✓	–	–	–	–
26-31	Service-Bundle	–	✓	–	–	–	–
26-33	Tunnel-Maximum-Sessions	–	✓	–	–	–	–
26-34	Framed-IP-Route-Tag	–	✓	–	–	–	–
26-47	Ipv6-Primary-DNS	–	✓	–	–	–	–
26-48	Ipv6-Secondary-DNS	–	✓	–	–	–	–
26-55	DHCP-Options	✓	–	–	–	–	–
26-56	DHCP-MAC-Address	✓	✓	–	–	–	–
26-57	DHCP-GI-Address	✓	–	–	–	–	–
26-58	LI-Action	–	✓	–	–	✓	–

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-59	Med-Dev-Handle	–	✓	–	–	✓	–
26-60	Med-Ip-Address	–	✓	–	–	✓	–
26-61	Med-Port-Number	–	✓	–	–	✓	–
26-63	Interface-Desc	✓	–	–	–	–	–
26-64	Tunnel-Group	–	✓	–	–	–	–
26-65	Activate-Service	–	✓	–	–	✓	–
26-66	Deactivate-Service	–	✓	–	–	✓	–
26-69	Service-Statistics	–	✓	–	–	✓	–
26-70	Ignore-DF-Bit	–	✓	–	–	–	–
26-71	IGMP-Access-Name	–	✓	–	–	–	–
26-72	IGMP-Access-Src-Name	–	✓	–	–	–	–
26-74	MLD-Access-Name	–	✓	–	–	–	–
26-75	MLD-Access-Src-Name	–	✓	–	–	–	–
26-77	MLD-Version	–	✓	–	–	–	–
26-78	IGMP-Version	–	✓	–	–	–	–
26–91	Tunnel-Switch-Profile	–	✓	–	–	–	–
26-97	IGMP-Immediate-Leave	–	✓	–	–	–	
26-100	MLD-Immediate-Leave	–	✓	–	–	–	–
26-106	IPv6-Ingress-Policy-Name	–	✓	–	–	–	–
26-107	IPv6-Egress-Policy-Name	–	✓	–	–	–	–
26-108	CoS-Parameter-Type	–	✓	–	–	✓	–
26-109	DHCP-Guided-Relay-Server	–	✓	–	–	–	–
26-110	Acc-Loop-Cir-Id	✓	–	–	–	–	–

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-111	Acc-Aggr-Cir-Id-Bin	✓	–	–	–	–	–
26-112	Acc-Aggr-Cir-Id-Asc	✓	–	–	–	–	–
26-113	Act-Data-Rate-Up	✓	–	–	–	–	–
26-114	Act-Data-Rate-Dn	✓	–	–	–	–	–
26-115	Min-Data-Rate-Up	✓	–	–	–	–	–
26-116	Min-Data-Rate-Dn	✓	–	–	–	–	–
26-117	Att-Data-Rate-Up	✓	–	–	–	–	–
26-118	Att-Data-Rate-Dn	✓	–	–	–	–	–
26-119	Max-Data-Rate-Up	✓	–	–	–	–	–
26-120	Max-Data-Rate-Dn	✓	–	–	–	–	–
26-121	Min-LP-Data-Rate-Up	✓	–	–	–	–	–
26-122	Min-LP-Data-Rate-Dn	✓	–	–	–	–	–
26-123	Max-Interlv-Delay-Up	✓	–	–	–	–	–
26-124	Act-Interlv-Delay-Up	✓	–	–	–	–	–
26-125	Max-Interlv-Delay-Dn	✓	–	–	–	–	–
26-126	Act-Interlv-Delay-Dn	✓	–	–	–	–	–
26-127	DSL-Line-State	✓	–	–	–	–	–
26-128	DSL-Type	✓	–	–	–	–	–
26-130	QoS-Set-Name	–	✓	–	–	–	–
26-140	Service-Interim-Account-Interval	–	✓	–	–	✓	–
26-141	Downstream-Calculated-QoS-Rate	✓	–	–	–	–	–
26-142	Upstream-Calculated-QoS-Rate	✓	–	–	–	–	–
26-143	Max-Clients-Per-Interface	–	✓	–	–	–	–

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-146	Cos-Scheduler-Pmt-Type	–	✓	–	–	✓	–
26-158	PPPoE-Padn	–	✓	–	–	–	–
26-160	Vlan-Map-ID	–	✓	–	–	–	–
26-161	IPv6-Delegated-Pool-Name	–	✓	–	–	–	–
26-162	Tx-Connect-Speed	✓	–	–	–	–	–
26-163	Rx-Connect-Speed	✓	–	–	–	–	–
26-173	Service-Activate-Type	–	✓	–	–	✓	–
26-174	Client-Profile-Name	–	✓	–	–	–	–
27	Session-Timeout	–	✓	–	✓	–	–
31	Calling-Station-ID	✓	–	–	–	✓	–
32	NAS-Identifier	✓	–	–	–	–	–
44	Acct-Session-ID	✓	–	–	–	✓	✓
61	NAS-Port-Type	✓	–	–	–	–	–
64	Tunnel-Type	–	✓	–	–	–	–
65	Tunnel-Medium-Type	–	✓	–	–	–	–
66	Tunnel-Client-Endpoint	–	✓	–	–	–	–
67	Tunnel-Server-Endpoint	–	✓	–	–	–	–
69	Tunnel-Password	–	✓	–	–	–	–
82	Tunnel-Assignment-Id	–	✓	–	–	–	–
83	Tunnel-Preference	–	✓	–	–	–	–
85	Acct-Interim-Interval	–	✓	–	–	–	–
87	NAS-Port-Id	✓	–	–	–	✓	–
88	Framed-Pool	–	✓	–	–	–	–

Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
90	Tunnel-Client-Auth-Id	–	✓	–	–	–	–
91	Tunnel-Server-Auth-Id	–	✓	–	–	–	–
96	Framed-Interface-ID	–	✓	–	–	–	–
97	Framed-IPv6-Prefix	–	✓	–	–	–	–
99	Framed-IPv6-Route	–	✓	–	–	–	–
100	Framed-IPv6-Pool	–	✓	–	–	–	–
101	Error-Cause	–	–	–	–	✓	✓
123	Delegated-IPv6-Prefix	–	✓	–	–	–	–
242	Ascend-Data-Filter	–	✓	–	–	✓	–

Related Documentation

- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 59
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 5
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 37
- Juniper Networks VSAs Supported by the AAA Service Framework on page 44

AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS

Table 12 on page 59 shows the RADIUS attributes and Juniper Networks VSAs support in AAA accounting messages. A checkmark in a column indicates that the message type supports that attribute.

Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
1	User-Name	✓	✓	✓	–	–
3	CHAP-Password	✓	–	–	–	–
4	NAS-IP-Address	✓	✓	✓	✓	✓

Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
5	NAS-Port	✓	✓	✓	–	–
6	Service-Type	✓	✓	✓	–	–
7	Framed-Protocol	✓	✓	✓	–	–
8	Framed-IP-Address	✓	✓	✓	–	–
9	Framed-IP-Netmask	✓	✓	✓	–	–
11	Filter-Id	–	✓	✓	–	–
22	Framed-Route	✓	✓	✓	–	–
25	Class	✓	✓	✓	–	–
26-10	Ingress-Policy-Name	✓	✓	✓	–	–
26-11	Egress-Policy-Name	✓	✓	✓	–	–
26-42	Input-Gigapackets	–	✓	✓	–	–
26-43	Output-Gigapackets	–	✓	✓	–	–
26-47	Ipv6-Primary-DNS	✓	✓	✓	–	–
26-48	Ipv6-Secondary-DNS	✓	✓	✓	–	–
26-51	Tunnel-Disconnect-Cause-Info	–	✓	–	–	–
26-55	DHCP-Options	✓	✓	✓	–	–
26-56	DHCP-MAC-Address	✓	✓	✓	–	–
26-57	DHCP-GI-Address	✓	✓	✓	–	–
26-63	Interface-Desc	✓	✓	✓	–	–
26-83	Service-Session	–	✓	✓	–	–
26-110	Acc-Loop-Cir-Id	✓	✓	✓	–	–
26-111	Acc-Aggr-Cir-Id-Bin	✓	✓	✓	–	–
26-112	Acc-Aggr-Cir-Id-Asc	✓	✓	✓	–	–

Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
26-113	Act-Data-Rate-Up	✓	✓	✓	–	–
26-114	Act-Data-Rate-Dn	✓	✓	✓	–	–
26-115	Min-Data-Rate-Up	✓	✓	✓	–	–
26-116	Min-Data-Rate-Dn	✓	✓	✓	–	–
26-117	Att-Data-Rate-Up	✓	✓	✓	–	–
26-118	Att-Data-Rate-Dn	✓	✓	✓	–	–
26-119	Max-Data-Rate-Up	✓	✓	✓	–	–
26-120	Max-Data-Rate-Dn	✓	✓	✓	–	–
26-121	Min-LP-Data-Rate-Up	✓	✓	✓	–	–
26-122	Min-LP-Data-Rate-Dn	✓	✓	✓	–	–
26-123	Max-Interlv-Delay-Up	✓	✓	✓	–	–
26-124	Act-Interlv-Delay-Up	✓	✓	✓	–	–
26-125	Max-Interlv-Delay-Dn	✓	✓	✓	–	–
26-126	Act-Interlv-Delay-Dn	✓	✓	✓	–	–
26-127	DSL-Line-State	✓	✓	✓	–	–
26-128	DSL-Type	✓	✓	✓	–	–
26-141	Downstream-Calculated-QoS-Rate	✓	✓	✓	–	–
26-142	Upstream-Calculated-QoS-Rate	✓	✓	✓	–	–
26-151	IPv6-Acct-Input-Octets	–	✓	✓	–	–
26-152	IPv6-Acct-Output-Octets	–	✓	✓	–	–
26-153	IPv6-Acct-Input-Packets	–	✓	✓	–	–
26-154	IPv6-Acct-Output-Packets	–	✓	✓	–	–
26-155	IPv6-Acct-Input-Gigawords	–	✓	✓	–	–

Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
26-156	IPv6-Acct-Output-Gigawords	–	✓	✓	–	–
26-162	Tx-Connect-Speed	✓	✓	✓	–	–
26-163	Rx-Connect-Speed	✓	✓	✓	–	–
26–177	Cos-Shaping-Rate	✓	✓	✓	–	–
31	Calling-Station-ID	✓	✓	✓	–	–
32	NAS-Identifier	✓	✓	✓	–	–
40	Acct-Status-Type	✓	✓	✓	✓	✓
41	Acct-Delay-Time	✓	✓	✓	✓	✓
42	Acct-Input-Octets	–	✓	✓	–	–
43	Acct-Output-Octets	–	✓	✓	–	–
44	Acct-Session-ID	✓	✓	✓	✓	✓
45	Acct-Authentic	✓	✓	✓	✓	✓
46	Acct-Session-Time	–	✓	✓	–	–
47	Acct-Input-Packets	–	✓	✓	–	–
48	Acct-Output-Packets	–	✓	✓	–	–
49	Acct-Terminate-Cause	–	✓	✓	–	–
52	Acct-Input-Gigawords	–	✓	✓	–	–
53	Acct-Output-Gigawords	–	✓	✓	–	–
55	Event-Timestamp	✓	✓	✓	✓	✓
61	NAS-Port-Type	✓	✓	✓	–	–
64	Tunnel-Type	✓	✓	✓	–	–
65	Tunnel-Medium-Type	✓	✓	✓	–	–
66	Tunnel-Client-Endpoint	✓	✓	✓	–	–

Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
67	Tunnel-Server-Endpoint	✓	✓	✓	–	–
82	Tunnel-Assignment-Id	✓	✓	✓	–	–
87	NAS-Port-Id	✓	✓	✓	–	–
90	Tunnel-Client-Auth-Id	✓	✓	✓	–	–
91	Tunnel-Server-Auth-Id	✓	✓	✓	–	–
99	Framed-IPv6-Route	✓	✓	✓	–	–
100	Framed-IPv6-Pool	✓	✓	✓	–	–
123	Delegated-IPv6-Prefix	✓	✓	✓	–	–

Related Documentation

- AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 54
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 5
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 37
- Juniper Networks VSAs Supported by the AAA Service Framework on page 44

DSL Forum Vendor-Specific Attributes

Digital Subscriber Line (DSL) attributes are RADIUS vendor-specific attributes (VSAs) that are defined by the DSL Forum. The attributes transport DSL information that is not supported by standard RADIUS attributes and which convey information about the associated DSL subscriber and data rate. The attributes are defined in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*.

NOTE: Junos OS uses the vendor ID 3561, which is assigned by the Internet Assigned Numbers Authority (IANA), for the DSL Forum VSAs.

Subscriber management does not process DSL values—the router simply passes the values received from the subscriber to the RADIUS server, without performing any parsing or manipulation. However, you can manage the content of DSL VSA values either by using the client configuration to restrict the DSL VSAs that the client sends, or by configuring the RADIUS server to ignore unwanted DSL VSAs.

Table 13 on page 64 describes the DSL Forum VSAs.

Table 13: DSL Forum VSAs

Attribute Number	Attribute Name	Description	Value
[26-1]	Agent-Circuit-Id	Identifier for the subscriber agent circuit ID that corresponds to the DSLAM interface from which subscriber requests are initiated	string
[26-2]	Agent-Remote-Id	Unique identifier for the subscriber associated with the DSLAM interface from which requests are initiated	string
[26-129]	Actual-Data-Rate-Upstream	Actual upstream data rate of the subscriber's synchronized DSL link	integer: 4-octet
[26-130]	Actual-Data-Rate-Downstream	Actual downstream data rate of the subscriber's synchronized DSL link	integer: 4-octet
[26-131]	Minimum-Data-Rate-Upstream	Minimum upstream data rate configured for the subscriber	integer: 4-octet
[26-132]	Minimum-Data-Rate-Downstream	Minimum downstream data rate configured for the subscriber	integer: 4-octet
[26-133]	Attainable-Data-Rate-Upstream	Upstream data rate that the subscriber can attain	integer: 4-octet
[26-134]	Attainable-Data-Rate-Downstream	Downstream data rate that the subscriber can attain	integer: 4-octet
[26-135]	Maximum-Data-Rate-Upstream	Maximum upstream data rate configured for the subscriber	integer: 4-octet
[26-136]	Maximum-Data-Rate-Downstream	Maximum downstream data rate configured for the subscriber	integer: 4-octet
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	Minimum upstream data rate in low power state configured for the subscriber	integer: 4-octet
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	Minimum downstream data rate in low power state configured for the subscriber	integer: 4-octet
[26-139]	Maximum-Interleaving-Delay-Upstream	Maximum one-way upstream interleaving delay configured for the subscriber	integer: 4-octet
[26-140]	Actual-Interleaving-Delay-Upstream	Subscriber's actual one-way upstream interleaving delay	integer: 4-octet
[26-141]	Maximum-Interleaving-Delay-Downstream	Maximum one-way downstream interleaving delay configured for the subscriber	integer: 4-octet

Table 13: DSL Forum VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value
[26-142]	Actual-Interleaving-Delay-Downstream	Subscriber's actual one-way downstream interleaving delay	integer: 4-octet
[26-144]	Access-Loop-Encapsulation	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated	string: 3-byte
[26-254]	IWF-Session	Indication that the interworking function (IWF) has been performed for the subscriber's session	No data field required

Related Documentation

- DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS on page 65

DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS

Table 14 on page 65 lists the DSL Forum VSAs supported by Junos OS in RADIUS Access-Request, Acct-Start, Acct-Stop, Interim-Acct, and CoA-Request messages. A checkmark in a column indicates that the message type supports that attribute. The DSL Forum vendor ID is 3561 (hexadecimal DE9), which is assigned by the IANA.

Table 14: DSL Forum VSAs—Supported RADIUS Messages

Attribute Number	Attribute Name	Access Request	Acct Start	Acct Stop	Interim Acct	CoA Request
[26-1]	Agent-Circuit-Id	✓	✓	✓	✓	✓
[26-2]	Agent-Remote-Id	✓	✓	✓	✓	✓
[26-129]	Actual-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-130]	Actual-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-131]	Minimum-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-132]	Minimum-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-133]	Attainable-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-134]	Attainable-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-135]	Maximum-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-136]	Maximum-Data-Rate-Downstream	✓	✓	✓	✓	–

Table 14: DSL Forum VSAs—Supported RADIUS Messages *(continued)*

Attribute Number	Attribute Name	Access Request	Acct Start	Acct Stop	Interim Acct	CoA Request
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	✓	✓	✓	✓	–
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	✓	✓	✓	✓	–
[26-139]	Maximum-Interleaving-Delay-Upstream	✓	✓	✓	✓	–
[26-140]	Actual-Interleaving-Delay-Upstream	✓	✓	✓	✓	–
[26-141]	Maximum-Interleaving-Delay-Downstream	✓	✓	✓	✓	–
[26-142]	Actual-Interleaving-Delay-Downstream	✓	✓	✓	✓	–
[26-144]	Access-Loop-Encapsulation	✓	✓	✓	✓	–
[26-254]	IWF-Session	✓	✓	✓	✓	–

Related Documentation

- DSL Forum Vendor-Specific Attributes on page 63

Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs

Table 15 on page 66 lists the RADIUS attributes and Juniper Networks VSAs and their corresponding Junos OS predefined variables that are used in dynamic profiles. When the router instantiates a dynamic profile following subscriber access, the Junos OS uses the predefined variable to specify the RADIUS attribute or VSA for the information obtained from the RADIUS server.

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
RADIUS Attribute			
Framed-IP-Address (8)	$junos-framed-route-ip-address	Address for the client	No
Filter-ID (11)	$junos-input-filter NOTE: Variable is also used for VSA 26–10.	Input filter to apply to client IPv4 interface	Yes
Framed-Route (22)	$junos-framed-route-ip-address-prefix	(Subattribute 1): Route prefix for access route	No
	$junos-framed-route-nexthop	(Subattribute 2): Next hop address for access route	No

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables *(continued)*

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	$junos-framed-route-cost	(Subattribute 3): Metric for access route	No
	$junos-framed-route-distance	(Subattribute 5): Preference for access route	No
	$junos-framed-route-tag	(Subattribute 6): Tag for access route	No
Framed-IPv6-Prefix (97)	$junos-ipv6-ndra-prefix	Prefix value in IPv6 Neighbor Discovery route advertisements	No
Framed-IPv6-Route (99)	$junos-framed-route-ipv6-address-prefix	(Subattribute 1): Framed IPv6 route prefix configured for the client	No
	$junos-framed-route-ipv6-cost	(Subattribute 3): Metric for access route	No
	$junos-framed-route-ipv6-distance	(Subattribute 5): Preference for access route	No
	$junos-framed-route-ipv6-nexthop	(Subattribute 2): IPv6 routing information configured for the client	No
	$junos-framed-route-ipv6-tag	(Subattribute 6): Tag for access route	No
Juniper Networks VSA			
Virtual-Router (26–1)	$junos-routing-instance	Routing instance to which subscriber is assigned	No
Ingress-Policy-Name (26–10)	$junos-input-filter NOTE: Variable is also used for RADIUS attribute 11.	Input filter to apply to client IPv4 interface	Yes
Egress-Policy-Name (26–11)	$junos-output-filter	Output filter to apply to client IPv4 interface	Yes
IGMP-Enable (26–23)	$junos-igmp-enable	Enable or disable IGMP on client interface	Yes

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables *(continued)*

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
IGMP-Access-Name (26–71)	$junos-igmp-access-group-name	Access list to use for the group (G) filter	Yes
IGMP-Access-Src-Name (26–72)	$junos-igmp-access-source-group-name	Access List to use for the source group (S,G) filter	Yes
MLD-Access-Name (26–74)	$junos-mld-access-group-name	Access list to use for the group (G) filter	Yes
MLD-Access-Src-Name (26–75)	$junos-mld-access-source-group-name	Access List to use for the source group (S,G) filter	Yes
MLD-Version (26–77)	$junos-mld-version	MLD protocol version	Yes
IGMP-Version (26–78)	$junos-igmp-version	IGMP protocol version	Yes
IGMP-Immediate-Leave (26–97)	$junos-igmp-immediate-leave	IGMP immediate leave	Yes
MLD-Immediate-Leave (26–100)	$junos-mld-immediate-leave	MLD immediate leave	Yes
IPv6-Ingress-Policy-Name (26–106)	$junos-input-ipv6-filter	Input filter to apply to client IPv6 interface	Yes
IPv6-Egress-Policy-Name (26–107)	$junos-output-ipv6-filter	Output filter to apply to client IPv6 interface	Yes
CoS-Traffic-Control-Profile-Parameter-Type (26–108)	$junos-cos-scheduler-map	(T01: Scheduler-map name) Name of scheduler map configured in traffic-control profile	Yes
	$junos-cos-shaping-rate	(T02: Shaping rate) Shaping rate configured in traffic-control profile	Yes
	$junos-cos-guaranteed-rate	(T03: Guaranteed rate) Guaranteed rate configured in traffic-control profile	Yes
	$junos-cos-delay-buffer-rate	(T04: Delay-buffer rate) Delay-buffer rate configured in traffic-control profile	Yes

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables *(continued)*

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	$junos-cos-excess-rate	(T05; Excess rate) Excess rate configured in traffic-control profile	Yes
	$junos-cos-traffic-control-profile	(T06: Traffic-control profile) Name of the traffic-control profile configured in a dynamic profile	Yes
	$junos-cos-shaping-mode	(T07; Shaping mode) CoS shaping mode configured in a dynamic profile	Yes
	$junos-cos-byte-adjust	(T08; Byte adjust) Byte adjustments configured for the shaping mode in a dynamic profile	Yes
	$junos-cos-adjust-minimum	(T09; Adjust minimum) Minimum adjusted value allowed for the shaping rate in a dynamic profile	Yes
	$junos-cos-excess-rate-high	(T10; Excess rate high) Excess rate configured for high-priority traffic in a dynamic profile	Yes
	$junos-cos-excess-rate-low	(T11; Excess rate low) Excess rate configured for low-priority traffic in a dynamic profile	Yes
	$junos-cos-shaping-rate-burst	(T12; Shaping rate burst) Burst size configured for the shaping rate in a dynamic profile	Yes
	$junos-cos-guaranteed-rate-burst	(T13; Guaranteed rate burst) Burst size configured for the guaranteed rate in a dynamic profile	Yes
Qos-Set-Name (26–130)	$junos-interface-set-name	Name of an interface set configured in a dynamic profile	Yes

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables *(continued)*

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
CoS-Scheduler-Pmt-Type (26–146)	$junos-cos-scheduler	(Null: Scheduler name) Name of scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-tx	(T01: CoS scheduler transmit rate) Transmit rate for scheduler configured in a dynamic profile	Yes Available for multiple parameters: • Percent • Rate
	$junos-cos-scheduler-bs	(T02: CoS scheduler buffer size) Buffer size for scheduler configured in a dynamic profile	Yes Available for multiple parameters: • Percent • Temporal
	$junos-cos-scheduler-pri	(T03: CoS scheduler priority) Packet-scheduling priority for scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-dropfile-low	(T04: CoS scheduler drop-profile low) Name of drop profile for RED loss-priority level **low** for scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-dropfile-medium-low	(T05: CoS scheduler drop-profile medium-low) Name of drop profile for RED loss-priority level **medium-low** for scheduler configured in a dynamic profile	Yes

Table 15: RADIUS Attributes and Corresponding Junos OS Predefined Variables *(continued)*

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	$junos-cos-scheduler-dropfile-medium-high	(T06: CoS scheduler drop-profile medium-high) Name of drop profile for RED loss-priority level **medium-high** for scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-dropfile-high	(T07: CoS scheduler drop-profile high) Name of drop profile for RED loss-priority level **high** for scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-dropfile-any	(T08: CoS scheduler drop-profile any) Name of drop profile for RED loss-priority level **any** for scheduler configured in a dynamic profile	Yes
	$junos-cos-scheduler-excess-rate	(T09: CoS scheduler excess rate) Excess rate configured for a scheduler in a dynamic profile	Yes Available for multiple parameters: • Percent • Proportion
	$junos-cos-scheduler-shaping-rate	(T10: CoS scheduler shaping rate) Shaping rate configured for a scheduler in a dynamic profile	Yes Available for multiple parameters: • Percent • Rate
	$junos-cos-scheduler-excess-priority	(T11: CoS scheduler excess priority) Excess priority configured for a scheduler in a dynamic profile	Yes

Related Documentation

- *Dynamic Variables Overview*
- *Configuring Predefined Dynamic Variables in Dynamic Profiles*
- *Junos OS Predefined Variables*

Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests

When a RADIUS-initiated CoA or disconnect operation is unsuccessful, the router includes an error-cause attribute (RADIUS attribute 101) in the CoA-NAK or Disconnect-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the message without an error-cause attribute. Table 16 on page 72 describes the error-cause codes.

Table 16: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
404	Invalid request	Some other aspect of the request is invalid, such as if one or more attributes are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the router.
504	Session context not removable	The subscriber identified by attributes in the request is owned by a component that is not supported.
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Related Documentation

- RADIUS-Initiated Change of Authorization (CoA) Overview on page 32
- RADIUS-Initiated Disconnect Overview on page 34

Mapping Application Terminate Reasons and RADIUS Terminate Codes

The Junos OS software uses default configuration mapping of terminate reasons for various protocols (AAA, DHCP, L2TP, and PPP) to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute, enabling you to provide different information about the cause of a termination.

When a AAA, DHCP, L2TP, or PPP session is terminated, the router logs a message for the internal terminate reason and logs another message for the RADIUS Acct-Terminate-Cause attribute (RADIUS attribute 49). RADIUS attribute 49 is also included in RADIUS Acct-Off and Acct-Stop messages. You can use the logged information to help monitor and troubleshoot terminated sessions.

NOTE: A single mapping for RADIUS account termination is shared by all clients.

Table 17 on page 73 lists the IETF RADIUS Acct-Terminate-Cause codes that you can use to map application terminate reasons. In addition, you can also configure and use proprietary codes for values beyond 22.

Table 17: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)
2	Lost Carrier	DCD was dropped on the port
3	Lost Service	Service can no longer be provided; for example, the user's connection to a host was interrupted
4	Idle Timeout	Idle timer expired
5	Session Timeout	Subscriber reached the maximum continuous time allowed for the service or session
6	Admin Reset	System administrator reset the port or session
7	Admin Reboot	System administrator terminated the session on the NAS; for example, prior to rebooting the NAS
8	Port Error	NAS detected an error on the port that required ending the session
9	NAS Error	NAS detected an error (other than on the port) that required ending the session
10	NAS Request	NAS ended the session for a non-error reason
11	NAS Reboot	NAS ended the session due to a non-administrative reboot
12	Port Unneeded	NAS ended the session because the resource usage fell below the low threshold; for example, the bandwidth-on-demand algorithm determined that the port was no longer needed
13	Port Preempted	NAS ended the session to allocate the port to a higher-priority use
14	Port Suspended	NAS ended the session to suspend a virtual session
15	Service Unavailable	NAS was unable to provide the requested service
16	Callback	NAS is terminating the current session in order to perform callback for a new session

Table 17: Supported RADIUS Acct-Terminate-Cause Codes *(continued)*

Code	Name	Description
17	User Error	An error in the user input caused the session to be terminated
18	Host Request	The login host terminated the session normally
19	Supplicant Restart	Supplicant state machine was reinitialized
20	Reauthentication Failure	A previously authenticated supplicant failed to reauthenticate successfully following expiration of the reauthentication timer or explicit reauthentication request by management action
21	Port Reinitialized	The port's MAC has been reinitialized
22	Port Administratively Disabled	The port has been administratively disabled

Related Documentation

- Configuring Custom Terminate Reason Mappings on page 100
- AAA Terminate Reasons on page 74
- DHCP Terminate Reasons on page 75
- L2TP Terminate Reasons on page 76
- PPP Terminate Reasons on page 92

AAA Terminate Reasons

Table 18 on page 74 lists the default AAA terminate mappings. The table indicates the supported AAA deny and shutdown reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 18: Default AAA Mappings

AAA Deny or Shutdown Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny address allocation failure	17	user error
deny no-resources	10	NAS request
deny server- request-timeout	17	user error

Table 18: Default AAA Mappings *(continued)*

AAA Deny or Shutdown Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
shutdown idle-timeout	4	idle timeout NOTE: For Junos release 13.1, the default mapping is to RADIUS accounting NAS Request (10) terminate cause.
shutdown session-timeout	5	session timeout NOTE: For Junos release 13.1, the default mapping is to RADIUS accounting NAS Request (10) terminate cause.
shutdown administrative-reset	6	admin reset
shutdown remote-reset	10	NAS request

NOTE: In Junos OS releases prior to releases 12.2R5, 12.3R3, and 13.2R1, the **idle-timeout** and **session-timeout** terminate reasons both had a default mapping to RADIUS accounting NAS Request (10) terminate cause. To support backward compatibility for these releases, you can configure the router to support the previous mapping by using the **terminate-code aaa shutdown (idle-timeout | session-timeout) radius 10** statement at the **[edit access]** hierarchy level.

Related Documentation

- Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 72
- Configuring Custom Terminate Reason Mappings on page 100

DHCP Terminate Reasons

Table 19 on page 76 lists the default DHCP terminate mappings. The table indicates the supported DHCP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 19: Default DHCP Mappings

DHCP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
nak	15	service unavailable
nas logout	10	NAS request
no offers	4	idle timeout
lost-carrier	2	session terminated / modem dropped DCD
client request	1	user request

Related Documentation

- Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 72
- Configuring Custom Terminate Reason Mappings on page 100

L2TP Terminate Reasons

Table 20 on page 76 lists the default L2TP terminate mappings. The table indicates the supported L2TP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 20: Default L2TP Mappings

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
issu in progress	9	NAS error
session access interface down	8	port error
session admin close	6	admin reset
session admin drain	6	admin reset
session call down	10	NAS request
session call failed	15	service unavailable
session create failed limit reached	9	NAS error
session create failed no resources	9	NAS error
session create failed single shot tunnel already fired	9	NAS error

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session create failed too busy	9	NAS error
session failover protocol resync disconnect	6	admin reset
session hardware unavailable	8	port error
session no resources server port	9	NAS error
session not ready	9	NAS error
session rx cdn	10	NAS request
session rx cdn avp bad hidden	10	NAS request
session rx cdn avp bad value assigned session id	10	NAS request
session rx cdn avp duplicate value assigned session id	10	NAS request
session rx cdn avp malformed bad length	10	NAS request
session rx cdn avp malformed truncated	10	NAS request
session rx cdn avp missing mandatory assigned session id	10	NAS request
session rx cdn avp missing mandatory result code	10	NAS request
session rx cdn avp missing random vector	10	NAS request
session rx cdn avp missing secret	10	NAS request
session rx cdn avp unknown	10	NAS request
session rx cdn no resources	10	NAS request
session rx iccn avp bad hidden	10	NAS request
session rx iccn avp bad value framing type	10	NAS request
session rx iccn avp bad value proxy authen type	10	NAS request
session rx iccn avp bad value unsupported proxy authen type	10	NAS request
session rx iccn avp malformed bad length	10	NAS request
session rx iccn avp malformed truncated	10	NAS request

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx iccn avp missing mandatory connect speed	10	NAS request
session rx iccn avp missing mandatory framing type	10	NAS request
session rx iccn avp missing mandatory proxy authen challenge	10	NAS request
session rx iccn avp missing mandatory proxy authen id	10	NAS request
session rx iccn avp missing mandatory proxy authen name	10	NAS request
session rx iccn avp missing mandatory proxy authen response	10	NAS request
session rx iccn avp missing random vector	10	NAS request
session rx iccn avp missing secret	10	NAS request
session rx iccn avp unknown	10	NAS request
session rx iccn no resources	10	NAS request
session rx iccn unexpected	10	NAS request
session rx icrp avp bad hidden	10	NAS request
session rx icrp avp bad value assigned session id	10	NAS request
session rx icrp avp duplicate value assigned session id	10	NAS request
session rx icrp avp malformed bad length	10	NAS request
session rx icrp avp malformed truncated	10	NAS request
session rx icrp avp missing mandatory assigned session id	10	NAS request
session rx icrp avp missing random vector	10	NAS request
session rx icrp avp missing secret	10	NAS request
session rx icrp avp unknown	10	NAS request
session rx icrp no resources	10	NAS request
session rx icrp unexpected	10	NAS request
session rx icrq admin close	6	admin reset

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx icrq authenticate failed host	10	NAS request
session rx icrq avp bad hidden	10	NAS request
session rx icrq avp bad value assigned session id	10	NAS request
session rx icrq avp bad value bearer type	10	NAS request
session rx icrq avp bad value cisco nas port	10	NAS request
session rx icrq avp duplicate value assigned session id	10	NAS request
session rx icrq avp malformed bad length	10	NAS request
session rx icrq avp malformed truncated	10	NAS request
session rx icrq avp missing mandatory assigned session id	10	NAS request
session rx icrq avp missing mandatory call serial number	10	NAS request
session rx icrq avp missing random vector	10	NAS request
session rx icrq avp missing secret	10	NAS request
session rx icrq avp unknown	10	NAS request
session rx icrq no resources	10	NAS request
session rx icrq unexpected	10	NAS request
session rx occn avp bad hidden	10	NAS request
session rx occn avp bad value framing type	10	NAS request
session rx occn avp malformed bad length	10	NAS request
session rx occn avp malformed truncated	10	NAS request
session rx occn avp missing mandatory connect speed	10	NAS request
session rx occn avp missing mandatory framing type	10	NAS request
session rx occn avp missing random vector	10	NAS request
session rx occn avp missing secret	10	NAS request

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx occn avp unknown	10	NAS request
session rx occn no resources	10	NAS request
session rx occn unexpected	10	NAS request
session rx ocrp avp bad hidden	10	NAS request
session rx ocrp avp bad value assigned session id	10	NAS request
session rx ocrp avp duplicate value assigned session id	10	NAS request
session rx ocrp avp malformed bad length	10	NAS request
session rx ocrp avp malformed truncated	10	NAS request
session rx ocrp avp missing mandatory assigned session id	10	NAS request
session rx ocrp avp missing random vector	10	NAS request
session rx ocrp avp missing secret	10	NAS request
session rx ocrp avp unknown	10	NAS request
session rx ocrp no resources	10	NAS request
session rx ocrp unexpected	10	NAS request
session rx ocrq admin close	10	admin reset
session rx ocrq authenticate failed host	10	NAS request
session rx ocrq avp bad hidden	10	NAS request
session rx ocrq avp bad value assigned session id	10	NAS request
session rx ocrq avp bad value bearer type	10	NAS request
session rx ocrq avp bad value framing type	10	NAS request
session rx ocrq avp duplicate value assigned session id	10	NAS request
session rx ocrq avp malformed bad length	10	NAS request
session rx ocrq avp malformed truncated	10	NAS request

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx ocrq avp missing mandatory assigned session id	10	NAS request
session rx ocrq avp missing mandatory bearer type	10	NAS request
session rx ocrq avp missing mandatory call serial number	10	NAS request
session rx ocrq avp missing mandatory called number	10	NAS request
session rx ocrq avp missing mandatory framing type	10	NAS request
session rx ocrq avp missing mandatory maximum bps	10	NAS request
session rx ocrq avp missing mandatory minimum bps	10	NAS request
session rx ocrq avp missing random vector	10	NAS request
session rx ocrq avp missing secret	10	NAS request
session rx ocrq avp unknown	10	NAS request
session rx ocrq no resources	10	NAS request
session rx ocrq unexpected	10	NAS request
session rx ocrq unsupported	9	NAS error
session rx sli avp bad hidden	10	NAS request
session rx sli avp bad value accm	10	NAS request
session rx sli avp malformed bad length	10	NAS request
session rx sli avp malformed truncated	10	NAS request
session rx sli avp missing mandatory accm	10	NAS request
session rx sli avp missing random vector	10	NAS request
session rx sli avp missing secret	10	NAS request
session rx sli avp unknown	10	NAS request
session rx sli no resources	10	NAS request
session rx unexpected packet lac incoming	10	NAS request

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx unexpected packet lac outgoing	10	NAS request
session rx unexpected packet lns incoming	10	NAS request
session rx unexpected packet lns outgoing	10	NAS request
session rx unknown session id	10	NAS request
session rx wen avp bad hidden	10	NAS request
session rx wen avp malformed bad length	10	NAS request
session rx wen avp malformed truncated	10	NAS request
session rx wen avp missing mandatory call errors	10	NAS request
session rx wen avp missing random vector	10	NAS request
session rx wen avp missing secret	10	NAS request
session rx wen avp unknown	10	NAS request
session rx wen no resources	10	NAS request
session timeout connection	10	NAS request
session timeout inactivity	4	idle timeout
session timeout session	5	session timeout
session timeout upper create	9	NAS error
session transmit speed unavailable	9	NAS error
session tunnel down	15	service unavailable
session tunnel failed	15	service unavailable
session tunnel switch profile deleted	6	admin reset
session tunneled interface down	8	port error
session unknown cause	9	NAS error
session upper create failed	9	NAS error

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session upper removed	15	service unavailable
session warmstart not operational	15	service unavailable
session warmstart recovery error	15	service unavailable
session warmstart upper not restacked	10	NAS request
tunnel admin close	6	admin reset
tunnel admin drain	6	admin reset
tunnel control channel failed	15	service unavailable
tunnel created no sessions	1	user request
tunnel destination address changed	6	admin reset
tunnel destination down	10	NAS request
tunnel failover protocol no resources for recovery tunnel	15	service unavailable
tunnel failover protocol no resources for session resync	15	service unavailable
tunnel failover protocol not supported	15	service unavailable
tunnel failover protocol not supported by peer	15	service unavailable
tunnel failover protocol recovery control channel failed	15	service unavailable
tunnel failover protocol recovery tunnel failed	15	service unavailable
tunnel failover protocol recovery tunnel finished	1	user request
tunnel failover protocol recovery tunnel primary down	1	user request
tunnel failover protocol session resync failed	15	service unavailable
tunnel host profile changed	6	admin reset
tunnel host profile deleted	6	admin reset
tunnel rx scccn authenticate failed challenge	17	user error
tunnel rx scccn avp bad hidden	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx scccn avp bad value challenge response	15	service unavailable
tunnel rx scccn avp malformed bad length	15	service unavailable
tunnel rx scccn avp malformed truncated	15	service unavailable
tunnel rx scccn avp missing challenge response	17	user error
tunnel rx scccn avp missing random vector	15	service unavailable
tunnel rx scccn avp missing secret	15	service unavailable
tunnel rx scccn avp unexpected challenge response	15	service unavailable
tunnel rx scccn avp unknown	15	service unavailable
tunnel rx scccn no resources	15	service unavailable
tunnel rx scccn session id not null	15	service unavailable
tunnel rx scccn unexpected	15	service unavailable
tunnel rx sccrp authenticate failed challenge	17	user error
tunnel rx sccrp authenticate failed host	17	user error
tunnel rx sccrp avp bad hidden	15	service unavailable
tunnel rx sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrp avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrp avp bad value challenge	15	service unavailable
tunnel rx sccrp avp bad value challenge response	15	service unavailable
tunnel rx sccrp avp bad value failover capability	15	service unavailable
tunnel rx sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx sccrp avp bad value protocol version	15	service unavailable
tunnel rx sccrp avp bad value receive window size	15	service unavailable
tunnel rx sccrp avp duplicate value assigned tunnel id	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrp avp malformed bad length	15	service unavailable
tunnel rx sccrp avp malformed truncated	15	service unavailable
tunnel rx sccrp avp missing challenge response	17	user error
tunnel rx sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrp avp missing mandatory host name	15	service unavailable
tunnel rx sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrp avp missing random vector	15	service unavailable
tunnel rx sccrp avp missing secret	15	service unavailable
tunnel rx sccrp avp unexpected challenge response	15	service unavailable
tunnel rx sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrp avp unknown	15	service unavailable
tunnel rx sccrp no resources	15	service unavailable
tunnel rx sccrp session id not null	15	service unavailable
tunnel rx sccrp unexpected	15	service unavailable
tunnel rx sccrq admin close	6	admin reset
tunnel rx sccrq authenticate failed host	17	user error
tunnel rx sccrq avp bad hidden	15	service unavailable
tunnel rx sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrq avp bad value challenge	15	service unavailable
tunnel rx sccrq avp bad value failover capability	15	service unavailable
tunnel rx sccrq avp bad value framing capabilities	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrq avp bad value protocol version	15	service unavailable
tunnel rx sccrq avp bad value receive window size	15	service unavailable
tunnel rx sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp malformed bad length	15	service unavailable
tunnel rx sccrq avp malformed truncated	15	service unavailable
tunnel rx sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrq avp missing mandatory host name	15	service unavailable
tunnel rx sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrq avp missing random vector	15	service unavailable
tunnel rx sccrq avp missing secret	15	service unavailable
tunnel rx sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrq avp unknown	15	service unavailable
tunnel rx sccrq bad address	15	service unavailable
tunnel rx sccrq no resources	15	service unavailable
tunnel rx sccrq no resources max tunnels	15	service unavailable
tunnel rx sccrq session id not null	15	service unavailable
tunnel rx sccrq unexpected	15	service unavailable
tunnel rx stopccn	1	user request
tunnel rx stopccn avp bad hidden	15	service unavailable
tunnel rx stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp malformed bad length	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx stopccn avp malformed truncated	15	service unavailable
tunnel rx stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx stopccn avp missing mandatory result code	15	service unavailable
tunnel rx stopccn avp missing random vector	15	service unavailable
tunnel rx stopccn avp missing secret	15	service unavailable
tunnel rx stopccn avp unknown	15	service unavailable
tunnel rx stopccn no resources	15	service unavailable
tunnel rx stopccn session id not null	15	service unavailable
tunnel rx frs avp malformed truncated	15	service unavailable
tunnel rx frs avp missing mandatory failover session state	15	service unavailable
tunnel rx frs avp missing random vector	15	service unavailable
tunnel rx frs avp missing secret	15	service unavailable
tunnel rx frs avp unknown	15	service unavailable
tunnel rx frs no resources	15	service unavailable
tunnel rx frs session id not null	15	service unavailable
tunnel rx fsq avp bad hidden	15	service unavailable
tunnel rx fsq avp malformed bad length	15	service unavailable
tunnel rx fsq avp malformed truncated	15	service unavailable
tunnel rx fsq avp missing mandatory failover session state	15	service unavailable
tunnel rx fsq avp missing random vector	15	service unavailable
tunnel rx fsq avp missing secret	15	service unavailable
tunnel rx fsq avp unknown	15	service unavailable
tunnel rx fsq no resources	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx fsq session id not null	15	service unavailable
tunnel rx fsr avp bad hidden	15	service unavailable
tunnel rx fsr avp malformed bad length	15	service unavailable
tunnel rx unexpected packet	15	service unavailable
tunnel rx unexpected packet for session	15	service unavailable
tunnel rx unknown packet message type indecipherable	15	service unavailable
tunnel rx unknown packet message type unrecognized	15	service unavailable
tunnel rx recovery scccn authenticate failed challenge	17	user error
tunnel rx recovery scccn avp bad hidden	15	service unavailable
tunnel rx recovery scccn avp bad value challenge response	15	service unavailable
tunnel rx recovery scccn avp malformed bad length	15	service unavailable
tunnel rx recovery scccn avp malformed truncated	15	service unavailable
tunnel rx recovery scccn avp missing challenge response	17	user error
tunnel rx recovery scccn avp missing random vector	15	service unavailable
tunnel rx recovery scccn avp missing secret	15	service unavailable
tunnel rx recovery scccn avp unexpected challenge response	15	service unavailable
tunnel rx recovery scccn avp unknown	15	service unavailable
tunnel rx recovery scccn no resources	15	service unavailable
tunnel rx recovery scccn session id not null	15	service unavailable
tunnel rx recovery sccrp authenticate failed challenge	17	user error
tunnel rx recovery sccrp avp bad hidden	15	service unavailable
tunnel rx recovery sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp bad value bearer capabilities	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrp avp bad value challenge	15	service unavailable
tunnel rx recovery sccrp avp bad value challenge response	15	service unavailable
tunnel rx recovery sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrp avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrp avp bad value suggested control sequence	15	service unavailable
tunnel rx recovery sccrp avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp malformed bad length	15	service unavailable
tunnel rx recovery sccrp avp malformed truncated	15	service unavailable
tunnel rx recovery sccrp avp mismatched host name	15	service unavailable
tunnel rx recovery sccrp avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrp avp missing challenge response	17	user error
tunnel rx recovery sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrp avp missing random vector	15	service unavailable
tunnel rx recovery sccrp avp missing secret	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge without secret	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrp avp unknown	15	service unavailable
tunnel rx recovery sccrp no resources	15	service unavailable
tunnel rx recovery sccrp session id not null	15	service unavailable
tunnel rx recovery sccrq admin close	6	admin reset
tunnel rx recovery sccrq avp bad hidden	15	service unavailable
tunnel rx recovery sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value challenge	15	service unavailable
tunnel rx recovery sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrq avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrq avp bad value tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp duplicate value tie breaker	15	service unavailable
tunnel rx recovery sccrq avp malformed bad length	15	service unavailable
tunnel rx recovery sccrq avp malformed truncated	15	service unavailable
tunnel rx recovery sccrq avp mismatched host name	15	service unavailable
tunnel rx recovery sccrq avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory host name	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp missing random vector	15	service unavailable
tunnel rx recovery sccrq avp missing secret	15	service unavailable
tunnel rx recovery sccrq avp missing tie breaker	15	service unavailable
tunnel rx recovery sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrq avp unknown	15	service unavailable
tunnel rx recovery sccrq no resources	15	service unavailable
tunnel rx recovery sccrq session id not null	15	service unavailable
tunnel rx recovery sccrq tunnel id not null	15	service unavailable
tunnel rx recovery stopccn avp bad hidden	15	service unavailable
tunnel rx recovery stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp malformed bad length	15	service unavailable
tunnel rx recovery stopccn avp malformed truncated	15	service unavailable
tunnel rx recovery stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp missing mandatory result code	15	service unavailable
tunnel rx recovery stopccn avp missing random vector	15	service unavailable
tunnel rx recovery stopccn avp missing secret	15	service unavailable
tunnel rx recovery stopccn avp unknown	15	service unavailable

Table 20: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery stopccn no resources	15	service unavailable
tunnel rx recovery stopccn session id not null	15	service unavailable
tunnel rx recovery unexpected packet	15	service unavailable
tunnel rx recovery unknown packet message type indecipherable	15	service unavailable
tunnel rx recovery unknown packet message type unrecognized	15	service unavailable
tunnel rx session packet null sid invalid	15	service unavailable
tunnel rx session packet null sid without assigned session id	15	service unavailable
tunnel timeout connection	15	service unavailable
tunnel timeout connection recovery tunnel	15	service unavailable
tunnel timeout idle	1	user request
tunnel unknown cause	9	NAS error
tunnel warmstart not operational	15	service unavailable
tunnel warmstart recovery error	15	service unavailable

Related Documentation

- Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 72
- Configuring Custom Terminate Reason Mappings on page 100

PPP Terminate Reasons

Table 21 on page 92 lists the default PPP terminate mappings. The table indicates the supported PPP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 21: Default PPP Mappings

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
admin logout	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
authenticate authenticator timeout	17	user error
authenticate challenge timeout	10	NAS request
authenticate chap no resources	10	NAS request
authenticate chap peer authenticator timeout	17	user error
authenticate deny by peer	17	user error
authenticate inactivity timeout	4	idle timeout
authenticate max requests	10	NAS request
authenticate no authenticator	10	NAS request
authenticate pap peer authenticator timeout	17	user error
authenticate pap request timeout	10	NAS request
authenticate session timeout	5	session timeout
authenticate too many requests	10	NAS request
authenticate tunnel fail immediate	10	NAS request
authenticate tunnel unsupported tunnel type	10	NAS request
bundle fail create	10	NAS request
bundle fail engine add	10	NAS request
bundle fail fragment size mismatch	10	NAS request
bundle fail fragmentation location	10	NAS request
bundle fail fragmentation mismatch	10	NAS request
bundle fail join	10	NAS request
bundle fail link selection mismatch	10	NAS request
bundle fail local mped not set yet	10	NAS request
bundle fail local mrru mismatch	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
bundle fail local mru mismatch	10	NAS request
bundle fail peer mrru mismatch	10	NAS request
bundle fail reassembly location	10	NAS request
bundle fail reassembly mismatch	10	NAS request
bundle fail record network	10	NAS request
bundle fail server location mismatch	10	NAS request
bundle fail static link	10	NAS request
failover during authentication	6	admin reset
interface admin disable	6	admin reset
interface down	2	lost carrier
interface no hardware	8	port error
ip admin disable	10	NAS request
ip inhibited by authentication	10	NAS request
ip link down	10	NAS request
ip max configure exceeded	10	NAS request
ip no local ip address	10	NAS request
ip no local ip address mask	10	NAS request
ip no local primary dns address	10	NAS request
ip no local primary nbns address	10	NAS request
ip no local secondary dns address	10	NAS request
ip no local secondary nbns address	10	NAS request
ip no peer ip address	10	NAS request
ip no peer ip address mask	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ip no peer primary dns address	10	NAS request
ip no peer primary nbns address	10	NAS request
ip no peer secondary dns address	10	NAS request
ip no peer secondary nbns address	10	NAS request
ip no service	10	NAS request
ip peer renegotiate rx conf ack	10	NAS request
ip peer renegotiate rx conf nak	10	NAS request
ip peer renegotiate rx conf rej	10	NAS request
ip peer renegotiate rx conf req	10	NAS request
ip peer terminate term ack	10	NAS request
ip peer terminate code rej	10	NAS request
ip peer terminate term req	10	NAS request
ip service disable	10	NAS request
ip stale stacking	10	NAS request
ipv6 admin disable	10	NAS request
ipv6 inhibited by authentication	10	NAS request
ipv6 link down	10	NAS request
ipv6 local and peer interface ids identical	10	NAS request
ipv6 max configure exceeded	10	NAS request
ipv6 no local ipv6 interface id	10	NAS request
ipv6 no peer ipv6 interface id	10	NAS request
ipv6 no service	10	NAS request
ipv6 peer renegotiate rx conf ack	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ipv6 peer renegotiate rx conf nak	10	NAS request
ipv6 peer renegotiate rx conf rej	10	NAS request
ipv6 peer renegotiate rx conf req	10	NAS request
ipv6 peer terminate code rej	10	NAS request
ipv6 peer terminate term ack	10	NAS request
ipv6 peer terminate term req	10	NAS request
ipv6 service disable	10	NAS request
ipv6 stale stacking	10	NAS request
lcp authenticate terminate hold	10	NAS request
lcp configured mrru too small	10	NAS request
lcp configured mru invalid	10	NAS request
lcp configured mru too small	10	NAS request
lcp dynamic interface hold	10	NAS request
lcp keepalive failure	10	NAS request
lcp loopback rx conf req	10	NAS request
lcp loopback rx echo reply	10	NAS request
lcp loopback rx echo req	10	NAS request
lcp max configure exceeded	10	NAS request
lcp mru changed	10	NAS request
lcp negotiation timeout	10	NAS request
lcp no localaccm	10	NAS request
lcp no localacfc	10	NAS request
lcp no local authentication	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp no local endpoint discriminator	10	NAS request
lcp no local magic number	10	NAS request
lcp no local mrru	10	NAS request
lcp no local mru	10	NAS request
lcp no localpfc	10	NAS request
lcp no peer accm	10	NAS request
lcp no peer authentication	10	NAS request
lcp no peer endpoint discriminator	10	NAS request
lcp no peer magicnumber	10	NAS request
lcp no peer mrru	10	NAS request
lcp no peer mru	10	NAS request
lcp no peer pfc	10	NAS request
lcp peer terminate code rej	1	user request
lcp peer terminate term ack	1	user request
lcp peer terminate term req	1	user request
lcp peer terminate protocol reject	1	user request
lcp peer renegotiate rx conf ack	1	user request
lcp peer renegotiate rx conf nak	1	user request
lcp peer renegotiate rx conf rej	1	user request
lcp peer renegotiate rx conf req	1	user request
lcp tunnel disconnected	10	NAS request
lcp tunnel failed	10	NAS request
link interface no hardware	8	port error

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lower interface attach failed	2	lost carrier
lower interface teardown	2	lost carrier
mpls admin disable	10	NAS request
mpls link down	10	NAS request
mpls max configure exceeded	10	NAS request
mpls no service	10	NAS request
mpls peer renegotiate rx conf ack	10	NAS request
mpls peer renegotiate rx conf nak	10	NAS request
mpls peer renegotiate rx conf rej	10	NAS request
mpls peer renegotiate rx conf req	10	NAS request
mpls peer terminate code rej	10	NAS request
mpls peer terminate term ack	10	NAS request
mpls peer terminate term req	10	NAS request
mpls service disable	10	NAS request
mpls stale stacking	10	NAS request
network interface admin disable	6	admin reset
no bundle	10	NAS request
no interface	8	port error
no link interface	8	port error
no ncps available	10	NAS request
no network interface	10	NAS request
no upper interface	9	NAS error
osi admin disable	10	NAS request

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
osi link down	10	NAS request
osi max configure exceeded	10	NAS request
osi no local align npdu	10	NAS request
osi no peer align npdu	10	NAS request
osi no service	10	NAS request
osi peer renegotiate rx conf ack	10	NAS request
osi peer renegotiate rx conf nak	10	NAS request
osi peer renegotiate rx conf rej	10	NAS request
osi peer renegotiate rx conf req	10	NAS request
osi peer terminate code rej	10	NAS request
osi peer terminate term ack	10	NAS request
osi peer terminate term req	10	NAS request
osi service disable	10	NAS request
osi stale stacking	10	NAS request
recovery active state cleanup	9	NAS error
recovery configured state cleanup	9	NAS error
recovery init state cleanup	9	NAS error
recovery terminated state cleanup	9	NAS error
recovery terminating state cleanup	9	NAS error
session init failed	9	NAS error
subscriber mgr activation failed	9	NAS error
subscriber mgr get credentials failed	9	NAS error
subscriber mgr link interface not found	9	NAS error

Table 21: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
subscriber mgr set state active failed	9	NAS error

Related Documentation

- Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 72
- Configuring Custom Terminate Reason Mappings on page 100

Configuring Custom Terminate Reason Mappings

Junos OS supports default configuration mapping of terminate reasons for various protocols (AAA, DHCP, L2TP, and PPP) to RADIUS Acct-Terminate-Cause attributes. When a AAA, DHCP, L2TP, or PPP session is terminated, the router logs a message for the internal terminate reason and logs another message for the RADIUS Acct-Terminate-Cause attribute (RADIUS attribute 49). RADIUS attribute 49 is also included in RADIUS Acct-Off and Acct-Stop messages.

You can create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute to provide different information about the cause of a termination.

To configure customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute:

1. Edit the **access** hierarchy.

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

2. Edit the **terminate-code** statement.

   NOTE: Terminate codes do not appear as options on platforms where they are not supported.

   ```
   [edit access]
   user@host# edit terminate-code
   ```

3. Specify the protocol option (aaa (deny | shutdown) | dchp | l2tp | ppp) that you want to modify.

   ```
   [edit access terminate-code]
   user@host# set protocol-option
   ```

4. Specify the terminate reason that you want to modify.

   ```
   [edit access terminate-code protocol-option]
   user@host# set term-reason
   ```

NOTE: Attempts to set a terminate reason mapping to its default value are rejected by the CLI.

5. Specify the RADIUS termination cause value (from 1 through 4294967295) that you want to use for the termination reason.

   [edit access terminate-code *protocol-option term-reason*]
   user@host# **set radius** ***term-cause***

NOTE: Deleting a customized mapping restores the default.

Related Documentation

- Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 72
- AAA Terminate Reasons on page 74
- DHCP Terminate Reasons on page 75
- L2TP Terminate Reasons on page 76
- PPP Terminate Reasons on page 92

CHAPTER 4

Domain Maps in Subscriber Access Networks

Domain Mapping Overview

Domain mapping enables you to configure a map that specifies access options and session-specific parameters. The map is based on the domain name of subscriber sessions — the router applies the mapped options and parameters to sessions for subscribers that have the specified domains. For example, you might configure a domain map that is based on the domain name **xyz.com**. The options and parameters in that domain map are then applied when subscribers with the specified domain name (for example, **bob@xyz.com**, **raj@xyz.com**, and **juan@xyz.com**) request an AAA service.

The domain map provides efficiency, and enables you to make changes for a large number of subscribers in one operation. For example, if an address assignment pool becomes exhausted due to the number of subscribers obtaining addresses from the pool, you can create a domain map that specifies that subscribers in a particular domain obtain addresses from a different pool. In another use of the domain map, you might create a new dynamic profile and then configure the domain map to specify which subscribers (by their domain) use that dynamic profile.

NOTE: Subscriber management is supported in the default logical system only. The documentation for the subscriber management domain mapping feature describes using the **aaa-logical-system** and **target-logical-system** statements to configure mapping to a non-default logical system. These statements are for future extensions of subscriber management and are not supported in current Junos OS releases.

Table 22 on page 104 describes the access options and parameters you can configure in the domain map.

Table 22: Domain Map Options and Parameters

Option	Description
AAA logical system/routing instance	Logical system/routing instance in which AAA sends authentication and accounting requests for the subscriber sessions. Subscriber management is supported in the default logical system only.
Access profile	Access profile applied to subscriber sessions.
Address pool	Address pool used to allocate addresses to subscribers.
Domain name rules	Rules for domain name usage, including domain name stripping, supported delimiters, and parse direction (delimiters and the parse direction are configured globally).
Dynamic profile	Dynamic profile applied to subscriber sessions.
PADN parameters	PPPoE route information for subscriber sessions.
Target logical system/routing instance	Logical system/routing instance to which the subscriber interface is attached. Subscriber management is supported in the default logical system only.
Tunnel profile	Tunnel profile applied to subscriber sessions.

Default Domain Map

You can configure a default domain map that the router uses for subscribers whose domain name does not explicitly match any existing domain map. The router also uses the default domain map when a subscriber username does not include a domain name.

You might configure the default domain map to provide limited feature support for guest subscribers, such as a specific address pool used for guests or the routing instance that provides AAA services. When the router is unable to match a subscriber request to a domain map, the router then uses the rules specified in the default domain map configuration to handle the subscriber request.

Related Documentation

- Configuring a Domain Map on page 153

PART 2

Configuration

CHAPTER 5

Configuration Tasks

Configuring Router or Switch Interaction with RADIUS Servers

You specify the RADIUS servers that the router or switch can use and you configure how the router or switch interacts with the servers. You can configure the router or switch to use multiple RADIUS servers on the network.

To specify a RADIUS server and how the router or switch interacts with the server:

1. Configure the IP address of the RADIUS server and specify that you want to configure the router or switch interaction with the server.

   ```
   [edit access]
   user@host# edit radius-server 192.168.1.250
   ```

2. (Optional) Configure the RADIUS server accounting port number. The default accounting port number is 1813.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set accounting-port 1813
   ```

3. (Optional) Configure the port number the router or switch uses to contact the RADIUS server. The default port number is 1812.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set port 18914
   ```

4. (Optional) Configure the number of times that the router or switch attempts to contact a RADIUS accounting server. You can configure the router or switch to retry from 1 through 16 times. The default setting is 3 retry attempts.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set retry 4
   ```

5. Configure the required secret (password) that the local router or switch passes to the RADIUS client. Secrets enclosed in quotation marks can contain spaces.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set secret $nt1UE1*7688+
   ```

6. (Optional) Configure the maximum number of outstanding requests that a RADIUS server can maintain. An outstanding request is a request to which the RADIUS server has not yet responded. You can limit the number from 0 through 2000 outstanding requests per RADIUS server. The default setting is 1000 outstanding requests per server.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set max-outstanding-requests 500
   ```

7. Configure the source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router or switch interfaces.

   ```
   [edit access radius-server 192.168.1.250]
   user@host# set source-address 192.168.1.100
   ```

8. (Optional) Configure the length of time that the local router or switch waits to receive a response from a RADIUS server. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius-server 192.168.1.250]
user@host# set timeout 45
```

Related Documentation

- AAA Service Framework Overview on page 3
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring Authentication and Accounting Parameters for Subscriber Access

You use an access profile to configure authentication and accounting support for the subscriber access management feature. The access profile enables you to specify the type of methods used for authentication and accounting. You can also configure how subscriber access management collects and uses accounting statistics.

To configure authentication and accounting for subscriber access:

1. Specify the authentication and accounting methods to use.

   See "Specifying the Authentication and Accounting Methods for Subscriber Access" on page 109.

2. Specify how accounting statistics are collected.

   See "Configuring Per-Subscriber Session Accounting" on page 110.

Related Documentation

- AAA Service Framework Overview on page 3
- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Specifying the Authentication and Accounting Methods for Subscriber Access

You can specify the authentication and accounting methods that subscriber access management uses.

You can configure multiple authentication and accounting methods—the **authentication-order** and **accounting order** statements specify the order in which the subscriber access management feature uses the methods. For example, an authentication entry of **radius password** specifies that RADIUS authentication is performed first and, if it fails, local authentication (**password**) is done.

You can specify the following authentication methods:

NOTE: For this release, you must always specify the **radius** authentication method. Subscriber access management does not support the **password** keyword (the default), and authentication fails when no method is specified.

- **password**—Local authentication
- **radius**—RADIUS-based authentication

You can specify the following accounting methods:

- **radius**—RADIUS-based accounting

To configure the authentication and accounting methods for subscriber access management:

1. Specify the authentication methods and the order in which they are used. For this release, only **radius** is supported.

   ```
   [edit access profile isp-bos-metro-fiber-basic]
   user@host# set authentication-order radius
   ```

2. Specify the accounting method.

   ```
   [edit access profile isp-bos-metro-fiber-basic]
   user@host# set accounting order radius
   ```

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Configuring Per-Subscriber Session Accounting on page 110
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring Per-Subscriber Session Accounting

To configure accounting for a subscriber session, you use an access profile, and specify how the subscriber access management feature collects and uses the accounting statistics. The router uses the RADIUS attributes and Juniper Networks VSAs discussed in "RADIUS Accounting Statistics for Subscriber Access Overview" on page 19 to provide the accounting statistics for the subscriber session.

To configure accounting for a subscriber session:

1. At the **[edit access profile *profile-name*]** hierarchy level, specify that you want to configure accounting.

   ```
   [edit access profile profile-name]
   user@host# edit accounting
   ```

2. (Optional) Configure AAA to issue an Acct-Stop message if the AAA server denies access to the subscriber.

   [edit access profile *profile-name* accounting]
   user@host# set accounting-stop-on-access-deny

3. (Optional) Configure AAA to send an Acct-Stop message if the subscriber fails AAA but is granted access by the AAA server.

   [edit access profile *profile-name* accounting]
   user@host# set accounting-stop-on-failure

4. (Optional) Configure the router or switch to send an Acct-Update message to the RADIUS accounting server when a CoA occurs.

   [edit access profile *profile-name* accounting]
   user@host# set coa-immediate-update

5. (Optional) Configure subscriber management to send the RADIUS accounting report to both the wholesaler and the retailer accounting servers.

   [edit access profile *profile-name* accounting]
   user@host# set duplication

6. (Optional) Configure the router to send the RADIUS accounting report to multiple accounting servers listed in access profiles in a nondefault VRF (LS:RI).

   [edit access profile *profile-name* accounting duplication-vrf]
   user@host# set vrf-name ***vrf-name***
   user@host# set access-profile-name ***profile-name***

7. (Optional) Configure the router or switch to send an Acct-Update message to the RADIUS accounting server when the router or switch receives a response (for example, an ACK or timeout) to the Acct-Start message.

   [edit access profile *profile-name* accounting]
   user@host# set immediate-update

8. (Optional) Configure the order in which multiple accounting methods are used.

   [edit access profile *profile-name* accounting]
   user@host# set order **[** ***accounting-order*** **]**

9. (Optional) Configure the types of statistics to gather. You can specify that the router or switch collect both volume and time statistics or only time statistics for subscriber sessions. When you change the type of statistics being collected, current subscribers continue to use the previous collection specification. Subscribers who log in after the change use the new specification.

   [edit access profile *profile-name* accounting]
   user@host# set statistics **(time | volume-time)**

10. (Optional) Override the default behavior and specify that, after a CoA action that changes the RADIUS Class attribute, accounting reports for the subscriber's service sessions continue to use the original Class attribute that was assigned when the service sessions were created. The new Class attribute value is used in accounting reports for the subscriber session only. By default, the accounting reports for both the subscriber session and the subscriber's service sessions use the new Class attribute value.

[edit access profile *profile-name* accounting]
user@host# set coa-no-override service-class-attribute

11. (Optional) Configure the number of minutes between accounting updates. You can configure an interval from 10 through 1440 minutes. All values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.

    [edit access profile *profile-name* accounting]
    user@host# set update-interval ***minutes***

12. (Optional) Configure the authd process to wait for an Acct-On-Ack response message from RADIUS before sending any new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

    [edit access profile *profile-name* accounting]
    user@host# set wait-for-acct-on-ack

13. (Optional) Configure the authd process to send an Acct-On message when the first RADIUS server is added to the access profile, and to send an Acct-Off message when the last RADIUS server is removed from the access profile. This configuration enables you to monitor whether the access profile has an active RADIUS server.

    [edit access profile *profile-name* accounting]
    user@host# set send-acct-status-on-config-change

Related Documentation

- RADIUS Accounting Statistics for Subscriber Access Overview on page 19
- Understanding RADIUS Accounting Duplicate Reporting on page 21
- Configuring Per-Service Session Accounting on page 112
- Retaining Authentication and Accounting Information During Session Startup on page 8
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring Per-Service Session Accounting

Subscriber management enables you to configure the router to collect statistics on a per-service session basis for subscribers. Per-service session accounting requires two operations. First, RADIUS must be configured to provide the name of the service, the accounting interval to use, and the type of statistics to collect (either time statistics or a combination of time and volume statistics). Second, if RADIUS VSA 26-69 is configured for time and volume statistics, you must also configure a firewall or fast update firewall filter that counts service packets—the service packet information provides the volume statistics.

The router uses the RADIUS attributes and Juniper Networks VSAs discussed in "RADIUS Accounting Statistics for Subscriber Access Overview" on page 19 to provide the accounting statistics for the subscriber session.

NOTE: The collection of time-only service statistics is supported for all service sessions. However, time and volume statistics are provided for only firewall and fast update firewall service sessions.

To configure the router to provide per-service accounting statistics:

1. Ensure that the required RADIUS VSAs are configured.

   See Table 23 on page 113 for the VSAs that the router uses for per-service accounting.

2. Configure the classic firewall filter or fast update filter to count the service packets.

   See "Configuring Service Packet Counting" on page 113.

Table 23: Juniper Networks VSAs Used for Per-Service Session Accounting

Attribute Number	Attribute Name	Description	Value
26-69	Service-Statistics	Enable or disable statistics for the service	• 0 = disable • 1 = enable time statistics • 2 = enable time and volume statistics
26-83	Service-Session	Service string sent in accounting stop and start messages from the router to the RADIUS server	string: service-name, with parameter values that are sent from RADIUS server in attribute 26-65.
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service	• range = 600–86400 seconds • 0 = disabled NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).

Related Documentation

- Configuring Service Packet Counting on page 113
- RADIUS Accounting Statistics for Subscriber Access Overview on page 19
- Configuring Per-Subscriber Session Accounting on page 110
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring Service Packet Counting

Subscriber management uses service packet counting to report volume statistics for subscribers on a per-service session basis. To configure service packet counting, you specify the accounting action, and subscriber management then applies the results to a specific named counter (__junos-dyn-service-counter) for use by RADIUS.

The accounting action you configure specifies the counting mechanism that subscriber management uses when capturing statistics—either inline counters or deferred counters. Inline counters are captured when the event occurs, and do not include any additional packet processing that might occur after the event. Deferred counters (also called accurate accounting) are not incremented until the packet is queued for transmission, and therefore include the entire packet processing. Deferred counters provide a more accurate count of the packets than inline counters, and are more useful for subscriber accounting and billing.

You configure the accounting mechanism by specifying either the **service-accounting-deferred** action (for deferred counters) or the **service-accounting** action (for inline counters) at the **[edit firewall family *family-name* filter *filter-name* term *term-name* then]** hierarchy level.

The two accounting mechanisms are mutually exclusive, both on a per-term basis and a per-filter basis. Also, both accounting actions are mutually exclusive with the count action on a per-term basis.

NOTE: You can define deferred counters for the inet and inet6 families for classic filters only. Fast update filters do not support deferred counters.

To enable service packet counting:

1. Configure any match conditions that you want to count using the service accounting action. For example:

   [edit firewall family inet filter *filtername* term *term-name*]
   user@host# **set from source-address *address***

2. Specify the accounting action for the filter.

   To use deferred counters:

   [edit firewall family inet filter *filtername* term *term-name*]
   user@host# **set then service-accounting-deferred**

   To use inline counters:

   [edit firewall family inet filter *filtername* term *term-name*]
   user@host# **set then service-accounting**

When the match conditions for the filter are met, the packet is counted and applied to the well-known service counter (__junos-dyn-service-counter) for use by the RADIUS server. This counter provides the volume statistics for per-service accounting.

TIP: You cannot use the **service-accounting** action or the **service-accounting-deferred** action in the same term as a **count** action.

Related Documentation

- *Classic Filters Overview*
- *Defining Dynamic Filter Processing Order*

- RADIUS Accounting Statistics for Subscriber Access Overview on page 19
- Configuring Per-Service Session Accounting on page 112
- Configuring Per-Subscriber Session Accounting on page 110
- *Guidelines for Configuring Firewall Filters*
- *Guidelines for Applying Firewall Filters*
- *Firewall Filter Terminating Actions*
- *Firewall Filter Nonterminating Actions*

Configuring Back-up Options for RADIUS Accounting

You can configure RADIUS accounting backup to preserve accounting data when the accounting server is unavailable because of a server or network outage. When backup is configured, RADIUS accounting stop messages are withheld and queued to be sent when connectivity is restored. You can specify the maximum number of stop messages that can be queued. When this maximum is reached, subsequent new subscriber logins fail because there is no remaining capacity to preserve accounting data for new sessions.

You can also configure how long the queued messages can be held. When this period expires, all pending accounting stops are flushed from the queue, even if the accounting server has come back online.

NOTE: Configuring accounting backup disables the revert timer. An error message is generated if you attempt to configure the revert-interval statement at the [edit access profile *profile-name* options] or [edit access radius-options] hierarchy levels.

CAUTION: Before you configure RADIUS accounting backup, ensure that RADIUS accounting and RADIUS authentication are configured on different servers. Subscriber authentication fails when the same server is configured for both authentication and accounting.

1. Enable accounting backup to use the default values.

   ```
   [edit access ]
   user@host# set accounting-backup-options
   ```

2. (Optional) Configure the number of accounting stops that the router can preserve while the accounting server is offline.

   ```
   [edit access accounting-backup-options]
   user@host# set max-pending-accounting-stops number
   ```

3. (Optional) Configure how long the router holds pending accounting stops before flushing them.

```
[edit access accounting-backup-options]
user@host# set max-withhold-time hold-time
```

For example, the following statements configure the backup options for all subscriber accounting; these statements specify that the router holds no more than 32,000 pending accounting stops—at which point all subsequent subscriber logins fail—and holds them no longer than 6 hours—at which point all pending messages are flushed and subscriber logins resume if they were failing:

```
[edit access accounting-backup-options]
user@host# set max-pending-accounting-stops 32000
user@host# set max-withhold-time 360
```

Related Documentation

- Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 22
- Forcing the Router to Contact the Accounting Server Immediately on page 116

Forcing the Router to Contact the Accounting Server Immediately

In the event of an accounting server outage while RADIUS accounting backup is enabled, by default the router waits for a time interval to expire before contacting the offline server. Rather than waiting for that interval to pass, you can force the router to immediately contact the server by issuing the **request network-access aaa replay pending-accounting-stops** command. The router sends a batch of pending accounting stop requests to the server. If the router receives an acknowledgment from the server, then the router continues to replay the pending messages to the server in batches at the periodic interval. If the router does not get that acknowledgment, then it resumes sending a single pending accounting stop message at the periodic interval.

To force the router to immediately contact the offline accounting server:

- Request the messages to be replayed.

  ```
  user@host> request network-access aaa replay pending-accounting-stops
  ```

Related Documentation

- Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 22

Configuring RADIUS Server Parameters for Subscriber Access

Include the **radius** statement at the **[edit access profile *profile-name*]** hierarchy level to specify the RADIUS parameters for the subscriber access manager feature. The following list provides an overview of the parameters you can configure:

- The IP addresses of one or more RADIUS authentication and accounting servers.

- Options for the RADIUS servers, such as the following:
  - Format (decimal or description) used for the accounting session
  - Method (round-robin or direct) the router or switch uses to communicate with the servers
  - NAS identifier to use for RADIUS requests
  - Revert time setting that specifies when the router or switch reverts to using the primary RADIUS server
  - Delimiter character and format for the NAS-Port-ID (RADIUS attribute 87) and Calling-Station-ID (RADIUS attribute 31)
- The RADIUS attributes to be ignored or excluded from RADIUS messages.

To configure RADIUS server parameters:

1. Specify that you want to configure RADIUS support.

   ```
   [edit access profile isp-bos-metro-fiber-basic]
   user@host# edit radius
   ```

2. Specify the addresses of RADIUS authentication and accounting servers.

   See "Specifying RADIUS Authentication and Accounting Servers for Subscriber Access" on page 117.

3. Configure the RADIUS server options.

   See "Configuring RADIUS Server Options for Subscriber Access" on page 118.

4. Configure RADIUS attributes that are ignored or excluded from RADIUS messages.

   See "Configuring How RADIUS Attributes Are Used for Subscriber Access" on page 129.

Related Documentation

- Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 117
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 129

Specifying RADIUS Authentication and Accounting Servers for Subscriber Access

You can specify one or more RADIUS authentication or accounting servers to use for subscriber access management.

To configure RADIUS authentication and accounting support:

1. Specify that you want to configure RADIUS support.

   ```
   [edit access profile isp-bos-metro-fiber-basic]
   user@host# edit radius
   ```

2. Specify the IP address of the RADIUS server used for authentication.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.251
```

3. Specify the IP address of the RADIUS server used for accounting.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set accounting-server 192.168.1.250
```

To configure multiple RADIUS authentication or accounting servers:

- Specify the IP addresses of all RADIUS servers used for authentication or accounting.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.251 192.168.1.252
user@host# set accounting-server 192.168.1.250 192.168.1.251
```

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 129
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring RADIUS Server Options for Subscriber Access

You can specify options that the router or switch uses when communicating with RADIUS authentication and accounting servers for subscriber access.

To configure RADIUS authentication and accounting server options:

1. Specify that you want to configure RADIUS.

```
[edit access profile isp-bos-metro-fiber-basic]
user@host# edit radius
```

2. Specify that you want to configure RADIUS options.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# edit options
```

3. (Optional) Configure the method the router or switch uses to access RADIUS accounting servers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set client-accounting-algorithm round-robin
```

4. (Optional) Configure the method the router or switch uses to access RADIUS authentication servers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set client-authentication-algorithm round-robin
```

5. (Optional) Configure the format the router or switch uses to identify the accounting session.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius options]
   user@host# set accounting-session-id-format decimal
   ```

6. (Optional) Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius options]
   user@host# set access-loop-id-local
   ```

7. (Optional) Specify the information that is excluded from the interface description that the router or switch passes to RADIUS for inclusion in RADIUS attribute 87 (NAS-Port-Id).

   ```
   [edit access profile isp-bos-metro-fiber-basic radius options]
   user@host# set interface-description-format exclude-adapter
   ```

8. (Optional) Configure the value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius options]
   user@host# set nas-identifier 56
   ```

9. (Optional) Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. The total of the widths must not exceed 32 bits, or the configuration fails.

   - For Ethernet subscribers:

     ```
     [edit access profile isp-bos-metro-fiber-basic radius options]
     user@host# set nas-port-extended-format ae-width 10 slot-width 4 adapter-width
       2 port-width 4 stacked-vlan-width 10 vlan-width 2
     ```

   - For ATM subscribers:

     ```
     [edit access profile retailer01 radius options]
     user@host# set nas-port-extended-format atm slot-width 3 adapter-width 2
       port-width 3 vpi-width 8 vci-width 16
     ```

10. (Optional) Configure the delimiter character that the router inserts between values in RADIUS attribute 87 (NAS-Port-ID).

    ```
    [edit access profile isp-bos-metro-fiber-basic radius options]
    user@host# set nas-port-id-delimiter %
    ```

11. (Optional) Configure the information that the router includes in RADIUS attribute 87 (NAS-Port-ID).

    ```
    [edit access profile isp-bos-metro-fiber-basic radius options]
    user@host# set nas-port-id-format agent-circuit-id agent-remote-id
    ```

12. (Optional) Configure the delimiter character that the router inserts between values in RADIUS attribute 31 (Calling-Station-ID).

    ```
    [edit access profile isp-bos-metro-fiber-basic radius options]
    user@host# set calling-station-id-delimiter "%"
    ```

13. (Optional) Configure the information that the router includes in RADIUS attribute 31 (Calling-Station-ID).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set calling-station-id-format agent-circuit-id agent-remote-id
```

14. (Optional) Configure the port type that is included in RADIUS attribute 61 (NAS-Port-Type). This specifies the port type the router uses to authenticate subscribers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-type ethernet wireless-ieee80211
```

NOTE: This statement is ignored if you configure the ethernet-port-type-virtual in the same access profile.

15. (Optional) Configure the router or switch to use a port type of **virtual** to authenticate clients.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set ethernet-port-type-virtual
```

NOTE: This statement takes precedence over the nas-port-type statement if you include both in the same access profile.

16. (Optional) Configure the number of seconds that the router or switch waits after a server has become unreachable.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set revert-interval 259200
```

17. (Optional) Specify that RADIUS attribute 5 (NAS-Port) includes the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set vlan-nas-port-stacked-format
```

18. (Optional) Configure the router to use the optional behavior when processing CoA requests that include changes to client profile dynamic variables.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set coa-dynamic-variable-validation
```

Related Documentation

- RADIUS Server Options for Subscriber Access on page 5
- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Manual Configuration of the NAS-Port-Type RADIUS Attribute on page 10
- Configuring a NAS-Port-ID with Additional Options on page 125
- Configuring a Calling-Station-ID with Additional Attributes on page 127
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring RADIUS Options for Subscriber Access Globally

You can configure RADIUS options that apply to all RADIUS servers globally.

To configure RADIUS options globally:

1. Specify that you want to configure RADIUS options.

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

2. (Optional) Configure the number of requests per second that the router can send to all the RADIUS servers collectively.

   ```
   [edit access radius-options]
   user@host# set request-rate 1000
   ```

3. (Optional) Configure the number of seconds that the router or switch waits after a server has become unreachable.

   ```
   [edit access radius-options]
   user@host# set revert-interval 86400
   ```

Related Documentation

- Global RADIUS Options for Subscriber Access on page 8
- request-rate on page 241
- revert-interval on page 243

Subscriber Access Interface Description Storage and Reporting Through RADIUS Overview

You can configure Junos OS to store subscriber access interface descriptions and report the interface description through RADIUS. This capability enables you to uniquely identify subscribers on a particular logical or physical interface. When you enable storing of the interface descriptions, RADIUS requests include the interface description in VSA 26-63, if the subscriber's access interface has been configured with an interface description. All interface descriptions must be statically configured using the Junos OS CLI. Storing and reporting of interface descriptions is supported for DHCP, PPP, and authenticated dynamic VLANS, and applies to any client session that either authenticates or uses the RADIUS accounting service. The description can contain letters, numbers, and hyphens (-), and can be up to 64 characters long.

You can enable or disable storage and reporting of interface descriptions as follows:

- To enable storing and reporting of interface descriptions, include the **report-interface-descriptions** statement at the **[edit access]** hierarchy level.
- To disable storing and reporting of interface descriptions, include the **radius attributes exclude** statement at the **[edit access profile *profile-name*** hierarchy level.

Interface Description Precedence

The interface description sent in the VSA depends on the configured interface. Two configuration models apply across topologies and protocols for subscriber management.

- Subscriber logical interface directly over a physical interface (non-underlying logical interfaces).
- Subscriber logical interface over an underlying logical interface and physical interface.

In both models, Junos OS selects the interface description to report based on order of precedence. Interfaces not configured with interface descriptions are excluded when selecting an interface by precedence. If no interface description is configured on any of the static interfaces in the subscriber interface hierarchy, VSA 26-63 is not sent in any of the RADIUS messages.

Example: Reporting Interface Descriptions on Non-Underlying Logical Interfaces

This topic shows an example of subscriber access with non-underlying logical interfaces. In this case, the logical interface can be a VLAN or a VLAN demux interface. This example shows a DHCP subscriber logical interface over a VLAN without a demux interface. For non-underlying interfaces, Junos OS selects which interface description to report based on the following order of precedence:

1. Logical interface description
2. Physical interface description

Based on the order of precedence that Junos OS uses to select the interface description for non-underlying interfaces, Junos OS reports subscriber_ifl_descr as the interface description.

```
system {
    services {
        dhcp-local-server {
            group LSG1 {
                authentication {
                    password radius;
                    username-include {
                        user-prefix rich;
                    }
                }
                }
                interface ge-1/0/0.100;
            }
        }
    }
}
interfaces {
    ge-1/0/0 {
        description subscriber_ifd_descr;
        vlan-tagging;
        unit 100 {
            description subscriber_ifl_descr;
            vlan-id 100;
            family inet {
                unnumbered-address lo0.0 preferred-source-address 100.20.0.1;
```

```
            }
        }
    }
}
```

Reporting Interface Descriptions on Underlying Logical Interfaces

Underlying logical interfaces can apply to both DHCP and PPP.

For DHCP, Junos OS selects which interface description to report based on the following order of precedence:

1. Underlying logical interface description
2. Underlying physical interface description

NOTE: For DHCP, Junos OS does not report the IP demux logical interface description.

For PPP over an underlying VLAN or VLAN demux interface, Junos OS selects which interface description to report based on the following order of precedence:

1. PPP interface description
2. Underlying VLAN without a demux interface or VLAN demux logical interface description
3. Underlying physical interface description

Example: PPP over an Underlying VLAN Demux Interface

The following example shows a PPP subscriber over an underlying VLAN demux interface. This configuration includes three possible interface descriptions. Based on the order of precedence that Junos OS uses to select the interface description for PPP, the interface description is reported as subscriber_ppp_ifl_descr_0.

```
interfaces {
    ge-1/0/0 {
        description subscriber_ifd_descr;
        hierarchical-scheduler maximum-hierarchy-levels 2;
        flexible-vlan-tagging;
    }
    demux0 {
        unit 0 {
            vlan-tags outer 1 inner 1;
            description subscriber_under_ifl_descr_1_1;
            demux-options {
                underlying-interface ge-1/0/0;
            }
            family pppoe {
                duplicate-protection;
            }
        }
        unit 1 {
            vlan-tags outer 1 inner 2;
            description subscriber_under_ifl_descr_1_2;
```

```
            demux-options {
                underlying-interface ge-1/0/0;
            }
            family pppoe {
                duplicate-protection;
            }
        }
    }
    pp0 {
        unit 0 {
            description subscriber_ppp_ifl_descr_0;
            ppp-options {
                chap;
                pap;
            }
            pppoe-options {
                underlying-interface demux0.0;
                server;
            }
        }
        unit 1 {
            description subscriber_ppp_ifl_descr_1;
            ppp-options {
                chap;
                pap;
            }
            pppoe-options {
                underlying-interface demux0.1;
                server;
            }
        }
    }
}
```

Interface Descriptions on Aggregated Ethernet Physical Interfaces

For aggregated Ethernet interfaces, the interface description on the aggregated Ethernet interface, for example AE0 or AE1, serves as the physical interface description.

Interface Descriptions on a Combination of Dynamic and Static Interfaces

If the subscriber's access is a combination of dynamic and static interfaces, Junos OS uses the description on the static interface.

Example: Reporting Interface Descriptions on Dynamic VLANs

If you create dynamic VLANs with authentication, Junos OS reports the interface description on the physical interface. In the following example, dynamic VLANs created over the ge-1/2/0 interface are authenticated with an interface description of ge-1/2/0-bos-mktg-group.

```
ge-1/2/0 {
    description ge-1/2/0-bos-mktg-group;
    flexible-vlan-tagging;
    auto-configure {
        vlan-ranges {
            dynamic-profile vlan-prof {
                accept inet;
                ranges {
```

```
                    any;
                }
            }
            authentication {
                password radius;
                username-include {
                    user-prefix rich;
                }
            }
        }
    }
}
```

Related Documentation

- report-interface-descriptions (Edit Access) on page 239
- exclude on page 207
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

Configuring a NAS-Port-ID with Additional Options

You can include optional values in the NAS-Port-ID (RADIUS attribute 87), which identifies the physical interface subscriber management uses to authenticate subscribers. By default, the NAS-Port-ID includes the **interface-description** value that describes the physical interface. You can include the following values in the NAS-Port-ID:

- **agent-circuit-id**
- **agent-remote-id**
- **interface-description**
- **nas-identifier**

To configure an access profile to provide additional options in the NAS-Port-ID:

1. Specify the access profile you want to configure.

   ```
   [edit]
   user@host# edit access profile retailer25
   ```

2. Specify that you want to configure RADIUS options.

   ```
   [edit access profile retailer25]
   user@host# edit radius options
   ```

3. Specify the character to use as the delimiter between the different attribute values in the NAS-Port-ID. By default, subscriber management uses the hash character (**#**).

   ```
   [edit access profile retailer25 radius options]
   user@host# set nas-port-delimiter %
   ```

4. Specify that you want to configure the format of the NAS-Port-ID.

   ```
   [edit access profile retailer25 radius options]
   user@host# edit nas-port-id-format
   ```

5. Include the interface description in the NAS-Port-ID. (The interface description is not included by default when you configure the **nas-port-id-format** statement.)

   ```
   [edit access profile retailer25 radius options nas-port-id-format]
   user@host# set interface-description
   ```

6. Include the Agent Circuit ID in the NAS-Port-ID.

   ```
   [edit access profile retailer25 radius options nas-port-id-format]
   user@host# set agent-circuit-id
   ```

7. Include the Agent Remote ID in the NAS-Port-ID.

   ```
   [edit access profile retailer25 radius options nas-port-id-format]
   user@host# set agent-remote-id
   ```

8. Include the NAS identifier value in the NAS-Port-ID.

   ```
   [edit access profile retailer25 radius options nas-port-id-format]
   user@host# set nas-identifier
   ```

Configuring a Calling-Station-ID with Additional Attributes

You can configure an alternative value for the Calling-Station-ID (RADIUS IETF attribute 31) in an access profile on the router.

By default, the Calling-Station-ID includes the **agent-circuit-id** string. Optionally, you can configure the Calling-Station-ID to include one or more of the following attributes, in any combination:

- Agent circuit identifier (**agent-circuit-id**)—String that uniquely identifies the subscriber's access node and the digital subscriber line (DSL) on the access node. The agent circuit identifier (ACI) string is stored in either the DHCP option 82 field of DHCP messages for DHCP traffic, or in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) control packets for PPPoE traffic.
- Agent remote identifier (**agent-remote-id**)—String that identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The agent remote identifier (ARI) string is stored in either the DHCP option 82 field for DHCP traffic, or in the DSL Forum Agent-Remote-ID VSA [26-2] for PPPoE traffic.
- Interface description (**interface-description**)—Description of the interface, which is not included in the Calling-Station-ID by default.
- NAS identifier (**nas-identifier**)—Name of the NAS that originated the authentication or accounting request. NAS-Identifier is RADIUS IETF attribute 32.

If you configure the format of the Calling-Station-ID with more than one optional value, a hash character (#) is the default delimiter that the router uses as a separator between the concatenated values in the resulting Calling-Station-ID string. Optionally, you can configure an alternative delimiter character for the Calling-Station-ID to use.

To configure an access profile to provide additional attributes in the Calling-Station-ID:

1. Specify the access profile you want to configure.

   ```
   [edit]
   user@host# edit access profile profile-name
   ```

2. Specify that you want to configure RADIUS options.

   ```
   [edit access profile profile-name]
   user@host# edit radius options
   ```

3. Specify the nondefault character to use as the delimiter between the different attribute values in the Calling-Station-ID.

   By default, subscriber management uses the hash character (**#**) as the delimiter in Calling-Station-ID strings that contain more than one optional value.

   ```
   [edit access profile profile-name radius options]
   user@host# set calling-station-id-delimiter delimiter-character
   ```

4. Configure the value for the NAS-Identifier (RADIUS attribute 32), which is used for authentication and accounting requests.

   ```
   [edit access profile profile-name radius options]
   user@host# set nas-identifier identifier-value
   ```

5. Specify that you want to configure the format of the Calling-Station-ID.

   ```
   [edit access profile profile-name radius options]
   user@host# edit calling-station-id-format
   ```

6. Include the interface description in the Calling-Station-ID.

   ```
   [edit access profile profile-name radius options calling-station-id-format]
   user@host# set interface-description
   ```

7. Include the agent circuit identifier in the Calling-Station-ID.

   ```
   [edit access profile profile-name radius options calling-station-id-format]
   user@host# set agent-circuit-id
   ```

8. Include the agent remote identifier in the Calling-Station-ID.

   ```
   [edit access profile profile-name radius options calling-station-id-format]
   user@host# set agent-remote-id
   ```

9. Include the configured NAS identifier value in the Calling-Station-ID.

   ```
   [edit access profile profile-name radius options calling-station-id-format]
   user@host# set nas-identifier
   ```

Example: Calling-Station-ID with Additional Attributes in an Access Profile

The following example creates an access profile named retailer01 that configures a Calling-Station-ID string that includes the NAS-Identifier (**fox**), interface description, agent circuit identifier, and agent remote identifier optional attributes.

```
[edit access profile retailer01 radius options]
nas-identifier "fox";
calling-station-id-delimiter "*";
calling-station-id format {
   nas-identifier;
   interface-description;
   agent-circuit-id;
   agent-remote-id;
}
```

The resulting Calling-Station-ID string is formatted as follows:

fox*ge-1/2/0.100:100*as007*ar921

where:

- The NAS-Identifier value is **fox**.
- The Calling-Station-ID delimiter character is ***** (asterisk).
- The interface description value is **ge-1/2/0.100:100**.

- The agent circuit identifier value is **as007**.
- The agent remote identifier value is **ar921**.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- RADIUS Server Options for Subscriber Access on page 5

Configuring How RADIUS Attributes Are Used for Subscriber Access

You can specify the attributes RADIUS ignores in RADIUS Access-Accept messages, and the attributes RADIUS excludes from specified message types.

To configure the attributes RADIUS ignores or excludes:

1. Specify that you want to configure RADIUS.

   ```
   [edit access profile isp-bos-metro-fiber-basic]
   user@host# edit radius
   ```

2. Specify that you want to configure how RADIUS attributes are ignored or excluded.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius]
   user@host# edit attributes
   ```

3. Specify the attributes you want RADIUS to ignore when the attributes are in Access-Accept messages. See Table 24 on page 129 for the attributes you can configure.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius attributes]
   user@host# set ignore input-filter output-filter
   ```

4. Configure RADIUS to exclude the specified attribute from the specified RADIUS message type. See Table 25 on page 130 for the attributes and message type combinations you can configure.

   ```
   [edit access profile isp-bos-metro-fiber-basic radius attributes]
   user@host# set exclude input-filter output-filter
   ```

You use the **ignore** statement to configure the router or switch to ignore a particular attribute in RADIUS Access-Accept messages. By default, the router or switch processes the attributes received from the external AAA server. Table 24 on page 129 lists the attributes supported in the **ignore** statement.

Table 24: Attributes That Can Be Ignored in RADIUS Access-Accept Messages

CLI Entry	Attribute Name	Attribute Number
dynamic-iflset-name	Interface-Set-Name	Juniper Networks VSA 26-130
framed-ip-netmask	Framed-Ip-Netmask	RADIUS attribute 9
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26–10
logical-system:routing-instance	Virtual-Router	Juniper Networks VSA 26–1

Table 24: Attributes That Can Be Ignored in RADIUS Access-Accept Messages *(continued)*

CLI Entry	Attribute Name	Attribute Number
output-filter	Egress-Policy-Name	Juniper Networks VSA 26–11

You use the **exclude** statement to configure the router or switch to exclude the specified attributes from the specified type of RADIUS message. Not all attributes appear in all types of RADIUS messages—the CLI indicates the RADIUS message type. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages. Table 25 on page 130 lists the attributes and message types supported in the **exclude** statement.

Table 25: Attributes That Can Be Excluded from RADIUS Messages

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
accounting-authentic	Acct-Authentic	RADIUS attribute 45	Accounting-On Accounting-Off
accounting-delay-time	Acct-Delay-Time	RADIUS attribute 41	Accounting-On Accounting-Off
accounting-session-id	Acct-Session-Id	RADIUS attribute 44	Access-Request Accounting-On Accounting-Off Accounting-Stop
accounting-terminate-cause	Acct-Terminate-Cause	RADIUS attribute 49	Accounting-Off
called-station-id	Called-Station-Id	RADIUS attribute 30	Access-Request Accounting-Start Accounting-Stop
calling-station-id	Calling-Station-Id	RADIUS attribute 31	Access-Request Accounting-Start Accounting-Stop
class	Class	RADIUS attribute 25	Accounting-Start Accounting-Stop
cos-shaping-rate	Cos-Shaping-Rate	Juniper Networks VSA 26-177	Accounting-Start Accounting-Stop

Table 25: Attributes That Can Be Excluded from RADIUS Messages *(continued)*

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
delegated-ipv6-prefix	Delegated-IPv6-Prefix	RADIUS attribute 123	Accounting-Start Accounting-Stop
dhcp-gi-address	DHCP-GI-Address	Juniper Networks VSA 26–57	Access-Request Accounting-Start Accounting-Stop
dhcp-mac-address	DHCP-MAC-Address	Juniper Networks VSA 26–56	Access-Request Accounting-Start Accounting-Stop
dhcp-options	DHCP-Options	Juniper Networks VSA 26–55	Access-Request Accounting-Start Accounting-Stop
downstream-calculated-qos-rate	Downstream-Calculated-QoS-Rate	Juniper Networks VSA 26-141	Access-Request Accounting-Start Accounting-Stop Interim-accounting
dsl-forum-attributes	Not applicable	Excludes the DSL Forum VSA (IANA vendor ID 3561)	Access-Request Accounting-Start Accounting-Stop Interim-accounting
dynamic-iflset-name	Qos-Set-Name	Juniper Networks VSA 26–130	Accounting-Start Accounting-Stop
event-timestamp	Event-Timestamp	RADIUS attribute 55	Accounting-On Accounting-Off Accounting-Start Accounting-Stop
filter-id	Filter-Id	RADIUS attribute 11	Accounting-Start Accounting-Stop

Table 25: Attributes That Can Be Excluded from RADIUS Messages *(continued)*

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
framed-ip-address	Framed-IP-Address	RADIUS attribute 8	Accounting-Start Accounting-Stop
framed-ip-netmask	Framed-IP-Netmask	RADIUS attribute 9	Accounting-Start Accounting-Stop
framed-ip-route	Framed-Route	RADIUS attribute 22	Accounting-Start Accounting-Stop
framed-ipv6-pool	Framed-IPv6-Pool	RADIUS attribute 100	Accounting-Start Accounting-Stop
framed-ipv6-prefix	Framed-IPv6-Prefix	RADIUS attribute 97	Accounting-Start Accounting-Stop
framed-ipv6-route	Framed-IPv6-Route	RADIUS attribute 99	Accounting-Start Accounting-Stop
framed-pool	Framed-Pool	RADIUS attribute 88	Accounting-Start Accounting-Stop
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26–10	Accounting-Start Accounting-Stop
input-gigapackets	Acct-Input-Gigapackets	Juniper Networks VSA 26–42	Accounting-Stop
input-gigawords	Acct-Input-Gigawords	RADIUS attribute 52	Accounting-Stop
input-ipv6-gigawords	IPv6-Acct-Input-Gigawords	Juniper Networks VSA 26–155	Accounting-Stop
input-ipv6-octets	IPv6-Acct-Input-Octets	Juniper Networks VSA 26–151	Accounting-Stop
input-ipv6-packets	IPv6-Acct-Input-Packets	Juniper Networks VSA 26–153	Accounting-Stop

Table 25: Attributes That Can Be Excluded from RADIUS Messages *(continued)*

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
interface-description	Interface-Desc	Juniper Networks VSA 26–53	Access-Request Accounting-Start Accounting-Stop
nas-identifier	NAS-Identifier	RADIUS attribute 32	Access-Request Accounting-on Accounting-off Accounting-Start Accounting-Stop
nas-port	NAS-Port	RADIUS attribute 5	Access-Request Accounting-Start Accounting-Stop
nas-port-id	NAS-Port-Id	RADIUS attribute 87	Access-Request Accounting-Start Accounting-Stop
nas-port-type	NAS-Port-Type	RADIUS attribute 61	Access-Request Accounting-Start Accounting-Stop
output-filter	Egress-Policy-Name	Juniper Networks VSA 26–11	Accounting-Start Accounting-Stop
ouput-gigapackets	Acct-Output-Gigapackets	Juniper Networks VSA 26–43	Accounting-Stop
output-gigawords	Acct-Output-Gigawords	RADIUS attribute 53	Accounting-Stop
output-ipv6-gigawords	IPv6-Acct-Output-Gigawords	Juniper Networks VSA 26–156	Accounting-Stop
output-ipv6-octets	IPv6-Acct-Output-Octets	Juniper Networks VSA 26–152	Accounting-Stop
output-ipv6-packets	IPv6-Acct-Output-Packets	Juniper Networks VSA 26–154	Accounting-Stop

Table 25: Attributes That Can Be Excluded from RADIUS Messages *(continued)*

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
upstream-calculated-qos-rate	Upstream-Calculated-QoS-Rate	Juniper Networks VSA 26-142	Access-Request Accounting-Start Accounting-Stop Interim-accounting

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 117
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 165

Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN

On MX Series routers with MPC/MIC interfaces, you can configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis. The router passes the NAS-Port-Type and NAS-Port attributes to the RADIUS server during the authentication, authorization, and accounting (AAA) process.

To configure the NAS-Port-Type and NAS-Port extended format on a per-physical interface, per-VLAN, or per-stacked VLAN basis, you must create a NAS-Port options definition, which includes the following components:

- NAS-Port-Type value—Specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.
- NAS-Port extended format—Configures the number of bits (bit width) for each field in the NAS-Port attribute, which specifies the physical port number of the NAS that is authenticating the subscriber. Fields in the NAS-Port attribute include: slot, adapter, port, VLAN, and S-VLAN. Optionally, you can also use the **stacked** option as part of the **nas-port-extended-format** statement to include S-VLAN IDs, in addition to VLAN IDs, in the extended format. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.
- VLAN ranges or S-VLAN ranges—Defines the VLAN range of subscribers or stacked VLAN range of subscribers to which each NAS-Port options definition applies.

NOTE: You can create a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 stacked VLAN ranges, but *cannot* include a combination of VLAN ranges and stacked VLAN ranges.

To configure the NAS-Port-Type and NAS-Port extended format on a per-physical interface, per-VLAN, or per-stacked VLAN basis:

1. Specify the physical interface you want to configure.
2. Enable VLAN tagging, stacked VLAN tagging, or flexible VLAN tagging on the interface.
   - For VLAN tagging, see *Enabling VLAN Tagging*.
   - For stacked VLAN tagging, see *Configuring Stacked VLAN Tagging*
   - For flexible VLAN tagging, also referred to as mixed tagging, see *Enabling VLAN Tagging*.
3. Specify that you want to configure RADIUS options for a physical interface, VLAN, or S-VLAN.

   [edit interfaces *interface-name*]
   user@host> **edit** radius-options

4. Create a named NAS-Port options definition.

   [edit interfaces *interface-name* radius-options]
   user@host# edit nas-port-options *nas-port-options-name*

5. Configure the NAS-Port-Type, and the VLAN ranges or stacked VLAN ranges to which the named NAS-Port options definition applies.

   - For per-physical interface configurations, see "Configuring the RADIUS NAS-Port-Type per Physical Interface" on page 137.
   - For per-VLAN configurations, see "Configuring the RADIUS NAS-Port-Type per VLAN" on page 138.
   - For per-stacked VLAN configurations, see "Configuring the RADIUS NAS-Port-Type per Stacked VLAN" on page 139.

6. Configure the NAS-Port extended format, and the VLAN ranges or stacked VLAN ranges to which the named NAS-Port options definition applies.

   - For per-physical interface configurations, see "Configuring the RADIUS NAS-Port Extended Format per Physical Interface" on page 141.
   - For per-VLAN configurations, see "Configuring the RADIUS NAS-Port Extended Format per VLAN" on page 143.
   - For per-stacked VLAN configurations, see "Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN" on page 144.

Related Documentation

- RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 12
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port-Type per Physical Interface

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-physical interface basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-physical interface basis is useful in network configurations that use a 1:1 access model or an N:1 access model.

To configure the NAS-Port-Type RADIUS attribute per physical interface:

1. Specify the interface you want to configure.

   [edit]
   user@host# **edit interfaces** ***interface-name***

2. Enable VLAN tagging on the interface.

   [edit interfaces *interface-name*]
   user@host# **set vlan-tagging**

   Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a physical interface.

   [edit interfaces *interface-name*]
   user@host# **edit** radius-options

4. Create a named NAS-Port options definition.

   [edit interfaces *interface-name* radius-options]
   user@host# **edit** nas-port-options ***nas-port-options-name***

5. Configure the NAS-Port-Type.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** nas-port-type ***port-type***

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** vlan-ranges (**any** | ***low-tag–high-tag***)

   Per-physical interface configurations typically require you to create a VLAN range that consists of all VLAN IDs on the physical interface. To do so, use the **any** option with the **vlan-ranges** statement.

The following example shows a per-interface NAS-Port options definition named subscribers-east that configures the **wireless-umts** NAS-Port-Type for a VLAN range consisting of all VLAN IDs on Gigabit Ethernet physical interface ge-1/0/0.

```
[edit interfaces ge-1/0/0 radius-options]
nas-port-options subscribers-east {
   nas-port-type wireless-umts;
   vlan-ranges {
```

```
        any;
    }
}
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port-Type per VLAN

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-VLAN basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-VLAN basis is useful in network configurations that use a 1:1 access model.

To configure the NAS-Port-Type RADIUS attribute per VLAN:

1. Specify the interface you want to configure.

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Enable VLAN tagging on the interface.

   ```
   [edit interfaces interface-name]
   user@host# set vlan-tagging
   ```

   Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a VLAN interface.

   ```
   [edit interfaces interface-name]
   user@host# edit radius-options
   ```

4. Create a named NAS-Port options definition.

   ```
   [edit interfaces interface-name radius-options]
   user@host# edit nas-port-options nas-port-options-name
   ```

5. Configure the NAS-Port-Type.

   ```
   [edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
   ```

```
user@host# set nas-port-type port-type
```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set vlan-ranges (any | low-tag–high-tag)
```

Per-VLAN configurations typically require you to create a VLAN range that consists of a single VLAN ID on the physical interface. To do so, set the ***low-tag*** and ***high-tag*** options in the **vlan-ranges** statement to the same value, as shown in the following example.

The following example shows a per-VLAN NAS-Port options definition named subscribers-west that configures the **ethernet** NAS-Port-Type for VLAN ID 3 on Gigabit Ethernet physical interface ge-1/1/0.

```
[edit interfaces ge-1/1/0 radius-options]
nas-port-options subscribers-west {
  nas-port-type ethernet;
  vlan-ranges {
    3-3;
  }
}
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port-Type per Stacked VLAN

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-stacked VLAN basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-stacked VLAN basis is useful in network configurations that use an N:1 access model.

To configure the NAS-Port-Type RADIUS attribute per stacked VLAN:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable stacked VLAN tagging on the interface.

   [edit interfaces *interface-name*]
   user@host# **set stacked-vlan-tagging**

   Setting stacked VLAN tagging enables you to configure dual VLAN tags for all logical interfaces on the physical interface. You must enable stacked VLAN tagging before you can configure the stacked VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a stacked VLAN interface.

   [edit interfaces *interface-name*]
   user@host# **edit** radius-options

4. Create a named NAS-Port options definition.

   [edit interfaces *interface-name* radius-options]
   user@host# **edit** nas-port-options ***nas-port-options-name***

5. Configure the NAS-Port-Type.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** nas-port-type ***port-type***

6. Configure the stacked VLAN range or ranges to which the NAS-Port options definition applies.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** stacked-vlan-ranges (**any** | ***low-outer-tag–high-outer-tag***),**any**

   Per-stacked VLAN configurations require you to create a stacked VLAN range of subscribers to which the NAS-Port options definition applies. You must configure the low and high outer tags (VLAN IDs) in the range 1 through 4094, and the inner tag (S-VLAN ID) as **any** to represent all S-VLAN ID tags.

7. Repeat Steps 3 through 6 to configure additional NAS-Port options definitions on this interface.

The following example creates two NAS-Port options definitions, subscribers-north and subscribers-south, configured on a per-stacked VLAN basis on Gigabit Ethernet physical interface ge-1/1/0.

The subscribers-north definition configures a NAS-Port-Type user-defined value (4711) for a stacked VLAN range with outer VLAN ID 1 and all inner S-VLAN IDs. The subscribers-south definition configures a NAS-Port-Type user-defined value (4722) for a stacked VLAN range with outer VLAN IDs in the range 2 through 10, and all inner S-VLAN IDs.

```
[edit interfaces ge-2/0/1 radius-options]
nas-port-options subscribers-north {
   nas-port-type 4711;
   stacked-vlan-ranges {
      1-1,any;
   }
}
   nas-port-options subscribers-south {
      nas-port-type 4722;
```

```
    stacked-vlan-ranges {
      2-10,any;
    }
  }
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port Extended Format per Physical Interface

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-physical interface basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-physical interface basis is useful in network configurations that use a 1:1 access model or an N:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per physical interface:

1. Specify the interface you want to configure.

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Enable VLAN tagging on the interface.

   ```
   [edit interfaces interface-name]
   user@host# set vlan-tagging
   ```

   Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a physical interface.

   ```
   [edit interfaces interface-name]
   user@host# edit radius-options
   ```

4. Create a named NAS-Port options definition.

   ```
   [edit interfaces interface-name radius-options]
   user@host# edit nas-port-options nas-port-options-name
   ```

5. Configure the NAS-Port extended format.

   ```
   [edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
   user@host# set nas-port-extended-format slot-width width adapter-width width
     port-width width vlan-width width
   ```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

   ```
   [edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
   user@host# set vlan-ranges (any | low-tag–high-tag)
   ```

   Per-physical interface configurations typically require you to create a VLAN range that consists of all VLAN IDs on the physical interface. To do so, use the **any** option with the **vlan-ranges** statement.

The following example shows a per-interface NAS-Port options definition named boston-subscribers that configures a NAS-Port extended format consisting of an 8-bit slot field, 8-bit adapter field, 8-bit port field, and 4-bit VLAN field. The boston-subscribers definition applies to a VLAN range consisting of all VLAN IDs on Gigabit Ethernet physical interface ge-2/0/1.

```
[edit interfaces ge-2/0/1 radius-options]
nas-port-options boston-subscribers {
  nas-port-extended-format {
    slot-width 8;
    adapter-width 8;
    port-width 8;
    vlan-width 4;
  }
  vlan-ranges {
    any;
  }
}
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port Extended Format per VLAN

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-VLAN basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-VLAN basis is useful in network configurations that use a 1:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per VLAN:

1. Specify the interface you want to configure.

   [edit]
   user@host# **edit interfaces** ***interface-name***

2. Enable VLAN tagging on the interface.

   [edit interfaces *interface-name*]
   user@host# **set vlan-tagging**

   Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a VLAN interface.

   [edit interfaces *interface-name*]
   user@host# **edit** radius-options

4. Create a named NAS-Port options definition.

   [edit interfaces *interface-name* radius-options]
   user@host# **edit** nas-port-options ***nas-port-options-name***

5. Configure the NAS-Port extended format.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** nas-port-extended-format **slot-width** ***width*** **adapter-width** ***width*** **port-width** ***width*** **vlan-width** ***width***

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** vlan-ranges (**any** | ***low-tag–high-tag***)

   Per-VLAN configurations typically require you to create a VLAN range that consists of a single VLAN ID on the physical interface. To do so, set the ***low-tag*** and ***high-tag*** options in the **vlan-ranges** statement to the same value, as shown in the following example.

The following example shows a per-VLAN NAS-Port options definition named paris-subscribers that configures a NAS-Port extended format consisting of a 4-bit slot field, 2-bit adapter field, 4-bit port field, and 2-bit VLAN field. The paris-subscribers definition applies to VLAN ID 1 on Gigabit Ethernet physical interface ge-1/0/1.

```
[edit interfaces ge-1/0/1 radius-options]
nas-port-options paris-subscribers {
  nas-port-extended-format {
    slot-width 4;
    adapter-width 2;
    port-width 4;
    vlan-width 2;
  }
  vlan-ranges {
    1-1;
  }
}
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 144

Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-stacked VLAN basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-stacked VLAN basis is useful in network configurations that use an N:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per stacked VLAN:

1. Specify the interface you want to configure.

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Enable stacked VLAN tagging on the interface.

   ```
   [edit interfaces interface-name]
   user@host# set stacked-vlan-tagging
   ```

   Setting stacked VLAN tagging enables you to configure dual VLAN tags for all logical interfaces on the physical interface. You must enable stacked VLAN tagging before you can configure the stacked VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a stacked VLAN interface.

   [edit interfaces *interface-name*]
   user@host# **edit** radius-options

4. Create a named NAS-Port options definition.

   [edit interfaces *interface-name* radius-options]
   user@host# **edit** nas-port-options ***nas-port-options-name***

5. Configure the NAS-Port extended format.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** nas-port-extended-format **slot-width** ***width*** **adapter-width** ***width*** **port-width** ***width*** **vlan-width** ***width*** **stacked**

   To include S-VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format, include the **stacked** option in the **nas-port-extended-format** statement.

6. Configure the stacked VLAN range or ranges to which the NAS-Port options definition applies.

   [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]
   user@host# **set** stacked-vlan-ranges (**any** | ***low-outer-tag–high-outer-tag***),**any**

   Per-stacked VLAN configurations require you to create a stacked VLAN range of subscribers to which the NAS-Port options definition applies. You must configure the low and high outer tags (VLAN IDs) in the range 1 through 4094, and the inner tag (S-VLAN ID) as **any** to represent all S-VLAN ID tags.

7. Repeat Steps 3 through 6 to configure additional NAS-Port options definitions on this interface.

The following example creates two NAS-Port options definitions, chicago-subscribers and barcelona-subscribers, configured on a per-stacked VLAN basis on Gigabit Ethernet physical interface ge-3/2/1.

The chicago-subscribers definition configures a NAS-Port extended format consisting of a 8-bit slot field, 8-bit adapter field, 8-bit port field, 4-bit stacked VLAN field, and 4-bit VLAN field. Because the **stacked** option is configured in this definition, S-VLAN IDs, in addition to VLAN IDs, are included in the extended format. The chicago-subscribers definition applies to a stacked VLAN range with outer VLAN ID 1, and all inner S-VLAN IDs.

The barcelona-subscribers definition configures a NAS-Port extended format consisting of a 8-bit slot field, 8-bit adapter field, 8-bit port field, 4-bit stacked VLAN field, and 4-bit VLAN field. Because the **stacked** option is *not* configured in this definition, S-VLAN IDs are not included in the extended format. The barcelona-subscribers definition applies to a stacked VLAN range with outer VLAN IDs in the range 2 through 10, and all inner S-VLAN IDs.

```
[edit interfaces ge-3/2/1 radius-options]
nas-port-options chicago-subscribers {
   nas-port-extended-format {
      slot-width 8;
      adapter-width 8;
      port-width 8;
```

```
      stacked-vlan-width 4;
      vlan-width 4;
      stacked;
    }
    stacked-vlan-ranges {
      1-1,any;
    }
  }
    nas-port-options barcelona-subscribers {
      nas-port-extended-format {
        slot-width 8;
        adapter-width 8;
        port-width 8;
        stacked-vlan-width 4;
        vlan-width 4;
      }
      stacked-vlan-ranges {
        2-10,any;
      }
    }
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14
- Configuring the RADIUS NAS-Port-Type per Physical Interface on page 137
- Configuring the RADIUS NAS-Port-Type per VLAN on page 138
- Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 139
- Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 141
- Configuring the RADIUS NAS-Port Extended Format per VLAN on page 143

Configuring the RADIUS NAS-Port Extended Format for ATM Interfaces

As an alternative to globally configuring an extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-physical interface basis for both Ethernet subscribers and ATM subscribers as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field of the NAS-Port attribute, including: slot, adapter, port, ATM virtual path identifier (VPI), and ATM virtual circuit identifier (VCI).

To configure the NAS-Port extended format for an ATM interface, include one or both of the following options in the **nas-port-extended-format** statement along with the other options as appropriate for your needs:

- **vpi-width**—Number of bits in the ATM VPI field, in the range 1 through 32
- **vci-width**—Number of bits in the ATM VCI field, in the range 1 through 32

NOTE: For ATM subscribers, the combined total of the widths of all fields must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.

To configure an extended format for the NAS-Port RADIUS attribute for an ATM interface:

1. Specify the ATM interface you want to configure.

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Specify that you want to configure RADIUS options for a physical interface.

   ```
   [edit interfaces interface-name]
   user@host# edit radius-options
   ```

3. Create a named NAS-Port options definition.

   ```
   [edit interfaces interface-name radius-options]
   user@host# edit nas-port-options nas-port-options-name
   ```

4. Configure the NAS-Port extended format.

   ```
   [edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
   user@host# set nas-port-extended-format slot-width width adapter-width width
     port-width width vpi-width width vci-width width
   ```

The following example shows a NAS-Port options definition named boston-subscribers for ATM interface at-1/0/4 that configures a NAS-Port extended format with an ATM slot width of 6 bits, ATM adapter width of 3 bits, ATM port width of 4 bits, ATM VPI width of 12 bits, and ATM VCI width of 24 bits.

```
[edit interfaces at-1/0/4 radius-options]
nas-port-options boston-subscribers {
   nas-port-extended-format {
      slot-width 6;
```

```
        adapter-width 3;
        port-width 4;
        vpi-width 12;
        vci-width 24;
    }
}
```

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- RADIUS Server Options for Subscriber Access on page 5
- Configuring RADIUS Server Options for Subscriber Access on page 118

Configuring RADIUS-Initiated Dynamic Request Support

The router uses the list of specified RADIUS authentication servers for both authentication and dynamic request operations. The router listens on UDP port 3799 for dynamic requests.

To configure RADIUS dynamic request support:

- Specify the IP address of the RADIUS server.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.3
```

To configure the router to support dynamic requests from more than one RADIUS server:

- Specify the IP addresses of multiple RADIUS servers.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.3 192.168.10.15
```

Related Documentation

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 31
- Dynamic Service Activation During Login Overview on page 32
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 32
- RADIUS-Initiated Disconnect Overview on page 34
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 5
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 72

CHAPTER 6

Configuration Tasks for Access Profiles

Configuring an Access Profile for Subscriber Management

Access profiles enable you to specify subscriber access authentication and accounting parameters. After access profiles are created, you can attach them at the **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]** hierarchy level or for use in automatically configuring VLANs or stacked VLANs at the **[edit interfaces *interface-name* auto-configure vlan-ranges]** or **[edit interfaces *interface-name* auto-configure stacked-vlan-ranges]** hierarchy levels.

To configure an access profile:

1. Edit the access stanza.

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

2. Specify an existing or new access profile name.

   ```
   [edit access]
   user@host# edit profile profile-name
   ```

3. Specify any desired subscriber access authentication and accounting parameters for the access profile.

Related Documentation

- Attaching Access Profiles on page 150
- *Configuring Dynamic Authentication for VLAN Interfaces*
- profile on page 231

Attaching Access Profiles

After you have created the access profile that specifies the subscriber access management authentication and accounting parameters, you can attach the profile. Subscriber access management supports attaching access profiles at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]**
- **[edit interfaces *interface-name* auto-configure vlan-ranges]**
- **[edit interfaces *interface-name* auto-configure stacked-vlan-ranges]**

To attach an access profile:

1. Edit the desired hierarchy level.

   ```
   [edit]
   user@host# edit logical-systems LS1 routing-instances RI1
   ```

2. Specify the name of the access profile that you want to attach.

   ```
   [edit logical-systems logical-system-name routing-instances routing-instance-name]
   user@host# set access-profile vz-bos-metro-fios-basic
   ```

Related Documentation

- AAA Service Framework Overview on page 3

Configuring DNS Name Server Addresses for Subscriber Management

This topic describes the procedure for configuring DNS name server addresses at the access profile and routing instance levels. For information about configuring addresses in DHCP address pools, see the DHCP topics referenced in the *Related Documentation* section. For information about configuring addresses on your RADIUS server, refer to your RADIUS software documentation. The order in which the name server configurations at different levels are preferred is described in "DNS Name Server Address Overview" on page 26.

BEST PRACTICE: In practice, choose either the domain-name-server statement or the domain-name-server-inet statement for IPv4 addresses. They both have the same effect and there is no need to use both statements. If you do use both statements, addresses configured with domain-name-server-inet are preferred over addresses configured with domain-name-server.

To configure DNS name server addresses globally:

1. Configure an IPv4 address.

   ```
   [edit access]
   user@host# set domain-name-server-inet dns-address
   ```

   Alternatively, you can use a different statement to configure an IPv4 address.

```
[edit access]
user@host# set domain-name-server dns-address
```

2. Configure an IPv6 address.

```
[edit access]
user@host# set domain-name-server-inet6 dns-address
```

For example, to configure multiple addresses of each type:

```
[edit access]
user@host# set domain-name-server-inet 172.16.25.31
user@host# set domain-name-server-inet 172.16.25.100
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:81ca
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:7334
```

To configure DNS name server addresses in an access profile:

1. Configure an IPv4 address.

```
[edit access profile profile-name]
user@host# set domain-name-server-inet dns-address
```

Alternatively, you can use a different statement to configure an IPv4 address.

```
[edit access profile profile-name]
user@host# set domain-name-server dns-address
```

2. Configure an IPv6 address.

```
[edit access profile profile-name]
user@host# set domain-name-server-inet6 dns-address
```

For example, to configure multiple addresses of each type:

```
[edit access profile vrf-s-access]
user@host# set domain-name-server-inet 172.20.10.01
user@host# set domain-name-server-inet 172.20.100.100
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:ac81
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:71bfd
```

Related Documentation

- DNS Name Server Address Overview on page 26
- *DHCP Attributes for Address-Assignment Pools*
- *Configuring DHCP Client-Specific Attributes*

Configuring Subscriber Session Options

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both. The subscriber session timeouts apply to both L2TP-tunneled and PPP-terminated subscriber sessions.

NOTE: To configure the timeout attributes in RADIUS, refer to the documentation for your RADIUS server.

To configure limitations on subscriber sessions:

1. Edit session options for the router access profile.

   ```
   [edit]
   user@host# edit access profile profile-name session-options
   ```

2. Configure the maximum period a subscriber session can be active.

   ```
   [edit access profile profile-name session-options]
   user@host# set client-session-timeout minutes
   ```

3. Configure the maximum period a subscriber session can be idle.

   ```
   [edit access profile profile-name session-options]
   user@host# set client-idle-timeout minutes
   ```

For example, to configure a client session timeout of 2 hours and an idle timeout of 15 minutes in the **acc-prof** profile:

```
[edit]
access {
  profile {
    acc-prof {
      session-options {
        client-session-timeout 120;
        client-idle-timeout 15;
      }
    }
  }
}
```

Related Documentation

- Understanding Session Options for Subscriber Access on page 27
- client-idle-timeout on page 197
- client-session-timeout on page 197

CHAPTER 7

Configuration Tasks for Domain Maps

Configuring a Domain Map

To configure a domain map for subscriber management:

1. Create the domain map. For the map name, specify the domain name that you want the domain map to use. (Use **default** for the name of the default domain map.)

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

   - For example, to create a domain map to be mapped to subscribers with the domain name **xyz.com**:

     ```
     [edit access]
     user@host# edit domain map xyz.com
     ```

   - To create a default domain map to be mapped to subscribers with non-matching domain names and subscribers without domain names:

     ```
     [edit access]
     user@host# edit domain map default
     ```

2. (Optional) Specify the access profile used to apply access rules for the domain map.

See "Specifying an Access Profile in a Domain Map" on page 154.

3. (Optional) For dynamic profiles, clarify the provided dynamic configuration for the subscriber session.

   See "Specifying a Dynamic Profile in a Domain Map" on page 156.

4. (Optional) Specify the address pool used to allocate address for the domain map.

   See "Specifying an Address Pool in a Domain Map" on page 155.

5. (Optional) Configure rules for domain names; for example; delimiters, parsing direction, and domain stripping. Delimiters and parsing direction are configured globally for all domain maps. Domain stripping is enabled in the domain map.

   See "Configuring Domain Name Usage for Domain Maps" on page 159.

6. (Optional) Assign a tunnel profile that provides tunnel definitions for the domain map.

   See "Specifying a Tunnel Profile in a Domain Map" on page 161.

7. (Optional) Assign a tunnel switch profile to be applied by the domain map.

   See "Specifying a Tunnel Switch Profile in a Domain Map" on page 162.

8. (Optional) Configure the PADN parameters used for PPPoE route information for the domain map.

   See "Configuring PADN Parameters for a Domain Map" on page 162.

Related Documentation

- Domain Mapping Overview on page 103
- Verifying and Managing Domain Map Configuration on page 268

Specifying an Access Profile in a Domain Map

You use access profiles to specify the access rules and options (for example, the RADIUS authentication server and attributes) that the router applies to subscriber sessions. The domain map feature enables you to apply a specific access profile for subscribers in a particular domain.

Access profiles can be specified or modified in several different ways. If conflicts occur, the router applies the access profiles based on the precedence rules shown in Table 26 on page 154.

Table 26: Precedence Rules for Applying Access Profiles

Precedence (High to Low)	How the Access Profile Is Applied
1	Specified by the RADIUS Redirect-VRouter-Name attribute (VSA 26-25)
2	Specified in the domain map configuration stanza
3	Indirectly specified in the domain map configuration stanza by the AAA logical system/routing instance mapping

Table 26: Precedence Rules for Applying Access Profiles *(continued)*

Precedence (High to Low)	How the Access Profile Is Applied
4	Specified in the client configuration stanza
5	Specified in the logical system/routing instance configuration stanza

To include an access profile in a domain map:

1. Specify the domain map you want to configure.

   [edit access]
   user@host# **edit domain map** ***domain-map-name***

2. Specify the access profile you want to include in the domain map.

   [edit access domain map *domain-map-name*]
   user@host# **set** access-profile ***profile-name***

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Specifying an Address Pool in a Domain Map

You can use the domain map feature to specify the address pool that the router uses to allocate address for subscriber sessions. The address pool can include both IPv4 and IPv6 address ranges.

Address pools can be specified or modified in several different ways. If conflicts occur, the router applies the address pool based on the precedence rules shown in Table 27 on page 155.

Table 27: Precedence Rules for Determining the Address Pool to Use

Precedence (High to Low)	How the Address Pool Reference Is Provided
1	Specified by the RADIUS Framed-Pool attribute (RADIUS attribute 88)
2	Configured in the domain map configuration stanza
3	Specified in the client configuration stanza (by address match rules)

To specify the address pool used for a domain map:

1. Specify the domain map you want to configure.

   [edit access]
   user@host# **edit domain map** ***domain-map-name***

2. Specify the address pool you want to use for the domain map.

   [edit access domain map *domain-map-name*]
   user@host# **set** address-pool ***pool-name***

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Specifying a Dynamic Profile in a Domain Map

A dynamic profile defines the set of characteristics that provide dynamic access and services for subscriber sessions (such as class-of-service, protocols, and interface support). The domain map feature enables you to apply a specific dynamic profile based on subscriber domains.

Dynamic profiles are configured at the **[edit dynamic-profiles]** hierarchy, and can be specified or modified in several different ways. If conflicts occur, the router applies the dynamic profiles based on the precedence rules shown in Table 28 on page 156.

Table 28: Precedence Rules for Applying Dynamic Profiles

Precedence (High to Low)	How the Dynamic Profile Is Applied
1	Specified by the RADIUS Virtual-Router attribute (VSA 26-1) or the Redirect-VRouter-Name attribute (VSA 26-25)
2	Specified in the domain map configuration stanza
3	Specified in the client configuration stanza

To include a dynamic profile in a domain map:

1. Specify the domain map you want to configure.

   [edit access]
   user@host# **edit domain map** ***domain-map-name***

2. Specify the dynamic profile you want to include in the domain map.

   [edit access domain map *domain-map-name*]
   user@host# **set** dynamic-profile ***profile-name***

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Specifying an AAA Logical System/Routing Instance in a Domain Map

By default a domain map uses the subscriber logical system/routing instance as the context in which the **authd** daemon sends AAA authentication and accounting requests. You can optionally configure the domain map to direct AAA requests to a particular

context based on the subscriber domain name. Specifying a non-default AAA context enables you to manage workflow and traffic load, and to efficiently make changes for a large number of subscribers. For example, after upgrading your RADIUS services, you might configure a domain map to specify that all subscribers in the domain **xyz.com** are now authenticated by a RADIUS server in a particular non-default AAA context.

NOTE: Changing the AAA context does not change the subscriber context. You use the target-logical-system command to explicitly configure the logical system/routing instance for subscribers.

To configure the default logical system and a non-default routing instance for AAA requests:

1. Specify the domain map you want to configure.

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

2. Specify the non-default routing instance. The AAA logical system is automatically set to the default.

   ```
   [edit access domain map domain-map-name]
   user@host# set aaa-routing-instance routing-instance-name
   ```

NOTE: Subscriber management is supported in the default logical system only. The following procedure, which describes configuring a non-default logical system, is for future extensions of subscriber management and is not supported in current Junos OS releases.

To configure a non-default logical system in which you want the **authd** daemon to send AAA requests:

1. Specify the domain map you want to configure.

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

2. Specify the logical system and optionally the non-default routing instance for AAA requests.

   - To configure a non-default logical system and default routing instance for AAA requests:

     ```
     [edit access domain map domain-map-name]
     user@host# set aaa-logical-system logical-system-name
     ```

   - To configure a non-default logical system and a non-default routing instance for AAA requests:

     ```
     [edit access domain map domain-map-name]
     user@host# set aaa-logical-system logical-system-name aaa-routing-instance
       routing-instance-name
     ```

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153
- Specifying a Target Logical System/Routing Instance in a Domain Map on page 158

Specifying a Target Logical System/Routing Instance in a Domain Map

By default, the router places a subscriber in the logical system/routing instance of the interface on which the subscriber negotiations start. Subscriber management can then use the authentication server or a domain map to change the subscriber's logical system/routing instance.

To use the domain map method, you configure the domain map to specify the target logical system and routing instance for the subscriber's interface. You can optionally configure the domain map to use the default logical system and a specific non-default routing instance.

To configure a default target logical system and a non-default routing instance for a subscriber's interface:

1. Specify the domain map you want to configure.

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

2. Specify the non-default target routing instance. The target logical system is automatically set to the default.

   ```
   [edit access domain map domain-map-name]
   user@host# set target-routing-instance routing-instance-name
   ```

NOTE: Subscriber management is supported in the default logical system only. The following procedure, which describes configuring a non-default target logical system, is for future extensions of subscriber management and is not supported in current Junos OS releases.

To configure a non-default target logical system for a subscriber's interface:

1. Specify the domain map you want to configure.

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

2. Specify the target logical system and, optionally, the non-default target routing instance for the subscriber's interface.

   - To configure a non-default target logical system and default target routing instance:

     ```
     [edit access domain map domain-map-name]
     user@host# set target-logical-system logical-system-name
     ```

   - To configure a non-default target logical system and a non-default target routing instance:

```
[edit access domain map domain-map-name]
user@host# set target-logical-system logical-system-name target-routing-instance
  routing-instance-name
```

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Configuring Domain Name Usage for Domain Maps

You can configure how the router determines domain names for the domain mapping feature. At the global level, you can specify rules that are used for domain maps. The global rules enable you to specify additional characters that the router can recognize as domain name delimiters and to specify the direction the router uses to parse domain names. At the domain map level, you can enable domain name stripping. Domain name stripping specifies that the router remove the domain name from the subscriber username prior to performing any additional processing for the domain map.

To configure domain name usage rules for domain maps:

1. (Optional) Configure the domain name delimiters you want the router to recognize for domain maps.

   See "Specifying Domain Name Delimiters" on page 159.

2. (Optional) Configure the parse direction you want the router to use when determining domain names for domain maps.

   See "Specifying the Parsing Direction for Domain Names" on page 160.

3. (Optional) Configure the router to remove the domain name from usernames in the domain map before using AAA services.

   See "Enabling Domain Name Stripping" on page 161.

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Specifying Domain Name Delimiters

A delimiter is the character that separates a subscriber username from the domain name. Delimiters are commonly used for domain name parsing or stripping. You can specify a maximum of eight delimiters that the router uses to recognize domain names for a domain map. If you do not configure any delimiters, the router uses the @ character by default.

For example, your network might include the subscribers **bob@abc.com**, **pete!xyz.com**, and **maria\pqr.com**. In this case, you configure the router to recognize the characters **@**, **!**, and **** as delimiters.

Keep the following guidelines in mind when specifying delimiters:

- You cannot use the semicolon (;) as a delimiter.
- If you configure optional delimiters, you must also specify the @ character (the default delimiter) if you want to continue to use it as a delimiter.
- If you configure optional delimiters and then unconfigure them, the router sets the domain map delimiter back to the default @ character.

To configure domain name delimiters for domain maps:

1. Specify that you want to configure domain attributes.

   ```
   [edit]
   user@host# edit access domain
   ```

2. Specify the characters you want to use as delimiters. Do not include spaces between the delimiters.

   ```
   [edit access domain]
   user@host# set delimiter [delimiter-character]
   ```

Related Documentation

- Configuring Domain Name Usage for Domain Maps on page 159

Specifying the Parsing Direction for Domain Names

You can specify the direction in which the router performs the parsing operation it uses to identify subscriber domain names for domain maps. During the parsing operation, the router searches the username until it recognizes a delimiter. It then considers anything to the right of the delimiter as the domain. By default, the router parses from right to left, starting at the right-most character in the username.

The parsing direction you use is important when there are nested domain names. For example, for the username **user1@abc.com@xyz.com**, right-to-left parsing produces a domain name of **xyz.com**. For the same username, left-to-right parsing produces a domain name of **abc.com@xyz.com**.

To configure the domain name parsing direction for domain maps:

1. Specify that you want to configure domain attributes.

   ```
   [edit]
   user@host# edit access domain
   ```

2. Specify the parsing direction you want the router to use.

   ```
   [edit access domain]
   user@host# set parse-direction (left-to-right | right-to-left)
   ```

Related Documentation

- Configuring Domain Name Usage for Domain Maps on page 159

Enabling Domain Name Stripping

You can configure the router to strip the domain name from usernames before any AAA services are used. Domain name stripping is done for domain maps. The router uses the delimiters and parsing direction you globally configure to determine the domain name that is removed. For example, if the router uses the default delimiter and parsing direction **right-to-left**, the username **user1@xyz.com** is stripped to be **user1**.

To configure the router to strip the domain name from usernames in a domain map:

1. Specify the domain map for the stripping operation.

   ```
   [edit]
   user@host# edit access domain map domain-map-name
   ```

2. Enable domain name stripping.

   ```
   [edit access domain map domain-map-name]
   user@host# set strip-domain
   ```

Related Documentation

- Configuring Domain Name Usage for Domain Maps on page 159

Specifying a Tunnel Profile in a Domain Map

Tunnel profiles specify tunnel definitions (for example, a set of L2TP tunnels and their attributes) that the router applies to subscriber sessions. The domain map feature enables you to apply a specific tunnel profile to subscribers in a particular domain.

NOTE: A tunnel profile specified by a RADIUS server in the Tunnel-Group attribute (VSA 26-64) takes precedence over the tunnel profile specified in the domain map.

To include a tunnel profile in a domain map:

1. Specify the domain map you want to configure.

   ```
   [edit access]
   user@host# edit domain map domain-map-name
   ```

2. Specify the tunnel profile you want to include in the domain map.

   ```
   [edit access domain map domain-map-name]
   user@host# set tunnel-profile profile-name
   ```

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153
- *Configuring a Tunnel Profile for Subscriber Access*

Specifying a Tunnel Switch Profile in a Domain Map

Tunnel switch profiles determine whether packets in an L2TP subscriber session from a LAC are switched to another session that has a different destination LNS. The tunnel switch profile can also specify how certain L2TP AVPs are handled when the packets are switched to a second tunnel. The domain map feature enables you to apply a specific tunnel switch profile to subscribers in a particular domain.

NOTE: A tunnel switch profile specified by a RADIUS server in the Tunnel-Group attribute (VSA 26-64) takes precedence over the tunnel switch profile specified in the domain map.

To include a tunnel switch profile in a domain map:

1. Specify the domain map you want to configure.

   [edit access]
   user@host# **edit domain map** ***domain-map-name***

2. Specify the tunnel switch profile you want to include in the domain map.

   [edit access domain map *domain-map-name*]
   user@host# **set tunnel-switch-profile** ***profile-name***

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153
- *Configuring L2TP Tunnel Switching*

Configuring PADN Parameters for a Domain Map

You can configure PPPoE to receive PPPoE Active Discovery Network (PADN) messages when a subscriber connects to a PPPoE server. The PADN information associates the PPPoE session with a set of routes that the session can use. You can configure the route information in a domain map, which enables you to apply specific PADN information to subscribers in a particular domain. You can configure a maximum of 16 routes in a domain map.

To configure PADN parameters in a domain map:

1. Specify the domain map you want to configure.

   [edit access]
   user@host# **edit domain map** ***domain-map-name***

2. Specify the PADN route information you want to include in the domain map. For each route, include the destination IP address, subnet mask, and route metric.

   [edit access domain map *domain-map-name*]
   user@host# **set** padn ***destination-address*** mask ***destination-mask*** metric ***route-metric***

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

CHAPTER 8

Examples

Example: Configuring RADIUS-Based Subscriber Authentication and Accounting

This example shows a RADIUS-based authentication and accounting configuration.

```
[edit access]
radius-server {
    192.168.1.250 {
        port 1812;
        accounting-port 1813;
        retry 3;
        secret &tIUEI*7688+;
        source-address 192.168.1.100;
        timeout 45;
    }
    192.168.1.251 {
        port 1812;
        accounting-port 1813;
        retry 3;
        secret $Dyu*UY(877-;
        source-address 192.168.1.100;
        timeout 30;
    }
    192.168.1.252 {
        port 1812;
```

```
        secret $Dyu*UY(877-;
    }
}
profile isp-bos-metro-fiber-basic {
    authentication-order radius;
    accounting {
        order radius;
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        immediate-update;
        statistics time;
        update-interval 12;
        wait-for-acct-on-ack;
        send-acct-status-on-config-change;
    }
    radius {
        authentication-server 192.168.1.251 192.168.1.252;
        accounting-server 192.168.1.250 192.168.1.251;
        options {
            accounting-session-id-format decimal;
            client-accounting-algorithm round-robin;
            client-authentication-algorithm round-robin;
            nas-identifier 56;
            nas-port-id-delimiter %;
            nas-port-id-format {
                nas-identifier;
                interface-description;
            }
            nas-port-type {
                ethernet {
                    wireless-80211;
                }
            }
        }
        attributes {
            ignore {
                framed-ip-netmask;
            }
            exclude {
                accounting-delay-time [accounting-start accounting-stop];
                accounting-session-id [access-request accounting-on accounting-off
                accounting-start accounting-stop];
                dhcp-gi-address [access-request accounting-start accounting-stop];
                dhcp-mac-address [access-request accounting-start accounting-stop];
                nas-identifier [access-request accounting-start accounting-stop];
                nas-port [accounting-start accounting-stop];
                nas-port-id [accounting-start accounting-stop];
                nas-port-type [access-request accounting-start accounting-stop];
            }
        }
    }
}
[edit logical-systems isp-bos-metro-12 routing-instances isp-cmbrg-12-32]
interfaces {
    lo0 {
        unit 0 {
```

```
        family inet {
          address 192.168.1.100/24;
        }
      }
    }
    ge-0/0/0 {
      vlan-tagging;
      unit 0 {
        vlan-id 200;
        family inet {
          unnumbered-address lo0.0;
        }
      }
    }
  }
```

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108

Example: Configuring an Address-Assignment Pool

This example shows an address-assignment pool configuration that creates two pools, one for IPv4 DHCP clients (**isp_1**) , and a second pool (**chi-fiber-ra**) that is used for router advertisement.

```
[edit access]
address-assignment {
  network-discovery-router-advertisement chi-fiber-ra;
  pool isp_1 {
    family inet {
      network 192.168.0.0/16;
      range southeast {
        low 192.168.102.2 high 192.168.102.254;
      }
      range northeast {
        low 192.168.119.2 high 192.168.119.250;
      }
      host svale6.boston.net {
        hardware-address 90:00:00:01:00:01;
        ip-address 192.168.44.12;
      }
      dhcp-attributes {
        option-match {
          option-82 {
            circuit-id fiber range northeast;
          }
          option-82 {
            circuit-id cable_net range southeast;
          }
        }
        boot-file boot.client;
        boot-server 192.168.200.100;
        grace-period 3600;
        maximum-lease-time 18000;
        netbios-node-type p-node;
```

```
            router 192.168.44.44 192.168.44.45;
          }
        }
      }
      pool chi-fiber-ra {
        family inet6 {
          prefix 2008:2009:2010::/48;
          range fiber3 {
            low 2008:2009:2010::1/64;
            high 2008:2009:2010::5/64;
          }
        }
      }
    }
```

This example creates an IPv4 address-assignment pool named **isp-1**, which contains two named address ranges, **southeast** and **northeast**. The address-assignment pool also contains a static binding for client **host sval6.boston.net**. The ISP_1 pool configuration also includes the **dhcp-attributes** statement, indicating that the pool is used for DHCP clients. If the option 82 **circuit-id** entry matches the string **fiber**, then DHCP assigns the client an address from the **northeast** range. If the option 82 **circuit-id** matches the string **cable_net**, DHCP assigns an address from the **southeast** range.

The second address-assignment pool created in this example is **chi-fiber-ra**. The **neighbor-discovery-router-advertisement** statement at the beginning of the syntax specifies that this named address-assignment pool is used for router advertisement. The syntax at the end of the example configures the address-assignment pool named **chi-fiber-ra**.

Related Documentation

- *Address-Assignment Pools Overview*
- *Configuring Address-Assignment Pools*
- *Configuring an Address-Assignment Pool for Router Advertisement*

Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first.**

Related Documentation

- *Extended DHCP Local Server Overview*

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
   group group_one {
      interface fe-0/0/2.0;
      interface fe-0/0/2.1;
   }
   group group_two {
      interface fe-0/0/3.0;
      interface fe-0/0/3.1;
   }
   pool-match-order {
      external-authority
      ip-address-first;
      option-82;
   }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

Related Documentation

- *Extended DHCP Local Server Overview*
- *Address-Assignment Pools Overview*

Example: Minimum DHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
   server-group {
      test 10.0.2.1;
   }
   active-server-group test;
```

```
    group all {
      interface fe-0/0/2.0;
    }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates a server group and an active server group named **test** with IP address 10.0.2.1. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Related Documentation

- *Extended DHCP Relay Agent Overview*

Example: DHCP Relay Agent Configuration with Multiple Clients and Servers

This example shows an extended DHCP relay agent configuration for a network that includes multiple DHCP clients and DHCP servers. Additional details follow the example.

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    sp-1 {
      10.0.2.1;
      10.0.2.2;
    }
    sp-2 {
      10.33.2.1;
      10.33.2.2;
      10.33.2.3;
    }
  }
  active-server-group sp-1;
  overrides layer2-unicast-replies;
  group clients_a {
    relay-option-82 circuit-id;
    interface fe-1/0/1.1;
    interface fe-1/0/1.2;
    interface fe-1/0/1.3;
  }
  group clients_b {
    relay-option-82 {
      circuit-id {
        prefix routing-instance-name;
      }
    }
    interface fe-1/0/1.4;
    interface fe-1/0/1.5;
    interface fe-1/0/1.6;
  }
  group eth_dslam_relay {
    active-server-group sp-2;
```

```
        overrides {
          trust-option-82;
          layer2-unicast-replies;
        }
        interface fe-1/0/1.7;
        interface fe-1/0/1.8;
        interface fe-1/0/1.9;
      }
    }
```

This example creates two server-groups: **sp-1**, which includes DHCP server addresses 10.0.2.1 and 10.0.2.2, and **sp-2**, which includes DHCP server addresses 10.33.2.1, 10.33.2.2, and 10.33.2.3. The active server group to which the DHCP relay agent configuration applies is **sp-1**. A global override is set that causes the DHCP relay agent to use Layer 2 unicast transmission to send DHCP reply packets from the DHCP server to DHCP clients during the discovery process.

The example also creates three groups of subscribers and their associated Fast Ethernet interfaces: **clients_a**, **clients_b**, and **eth_dslam_relay**. These groups are configured to meet different needs, as follows:

- The **clients_a** and **clients_b** groups consist of basic subscribers. The service provider for these groups inserts option 82 information in the DHCP packets that are destined for the DHCP server.
- The subscribers in **eth_dslam_relay** are connected to an Ethernet digital subscriber line access multiplexer (DSLAM) that functions as a Layer 2 DHCP relay agent. The active server group for **eth_dslam_relay** is **sp-2**. Overrides are set for the **eth_dslam_relay** group that enable the DHCP relay agent to trust option 82 information and to use Layer 2 unicast transmission to send DHCP reply packets to DHCP clients during discovery.

Related Documentation

- *Extended DHCP Relay Agent Overview*

Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or EX Series Switches
- Junos OS Release 12.3 or later or Junos OS Release 12.3R2 for EX Series switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.

  See *Extended DHCP Relay Agent Overview*.

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.

  See *Grouping Interfaces with Common DHCP Configurations*.

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

Configuration

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

- Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings on page 173
- Results on page 173

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group
  servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal fffff
  local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

1. Specify that you want to configure DHCP relay agent support.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option option-number 60
```

3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group
  servergroup-15
```

6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal fffff local-server-group
  servergroup-east
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  relay-option {
    option-number 60;
    equals {
      ascii video-gold {
        forward-only;
      }
```

```
        }
        equals {
          ascii video-bronze {
            local-server-group servergroup-15;
          }
        }
        default-action {
          drop;
        }
        starts-with {
          hexadecimal fffff {
            local-server-group servergroup-east;
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To verify the status of DHCP relay agent selective traffic processing, perform this task:

- Verifying the Status of DHCP Relay Agent Selective Traffic Processing on page 174

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose Verify the DHCP relay agent selective traffic processing status.

Action Display statistics for DHCP relay agent.

```
user@host> show dhcp relay statistics
Packets dropped:
    Total                       30
    Bad hardware address        1
    Bad opcode                  1
    Bad options                 3
    Invalid server address      5
    No available addresses      1
    No interface match          2
    No routing instance match   9
    No valid local address      4
    Packet too short            2
    Read error                  1
    Send error                  1
    Option 60                   1
    Option 82                   2

Messages received:
    BOOTREQUEST                 116
    DHCPDECLINE                 0
    DHCPDISCOVER                11
    DHCPINFORM                  0
    DHCPRELEASE                 0
    DHCPREQUEST                 105

Messages sent:
    BOOTREPLY                   0
    DHCPOFFER                   2
    DHCPACK                     1
    DHCPNAK                     0
    DHCPFORCERENEW              0

Packets forwarded:
    Total                       4
    BOOTREQUEST                 2
    BOOTREPLY                   2
```

Meaning The **Packets forwarded** field in the **show dhcp relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of **BOOTREQUEST** and **BOOTREPLY** packets forwarded.

Related Documentation

- *Extended DHCP Relay Agent Overview*
- *DHCP Options and Selective Traffic Processing Overview*
- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*
- *Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings*
- Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing on page 176

Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing

This example shows how to configure named interface group-based support for DHCPv6 relay agent selective processing, which uses DHCP option strings to identify, filter, and process client traffic.

This example describes DHCPv6 relay agent configuration—you can configure the related procedure for DHCP relay agent groups at the **[edit forwarding-options dhcp-relay]** hierarchy level. DHCPv6 selective processing supports DHCPv6 options 15 and 16. DHCP selective processing supports option 60 (MX Series routers only) and option 77.

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or PTX Series Packet Transport Routers
- Junos OS Release 12.3 or later.

Before you configure DHCPv6 relay agent selective processing support, be sure you:

- Configure DHCPv6 relay agent.

  See *Extended DHCP Relay Agent Overview* and *DHCPv6 Relay Agent Overview*.
- Configure the DHCPv6 named interface groups used for the configuration.

  See *Grouping Interfaces with Common DHCP Configurations*.
- Configure the DHCPv6 server groups used for the processing actions.

  See *Grouping Interfaces with Common DHCP Configurations*.

Overview

In this example, you configure group-level DHCPv6 relay agent named interface support for selective processing of client packets based on DHCPv6 option strings. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCPv6 option that DHCPv6 relay agent uses to identify the client traffic you want to process. The DHCPv6 option you specify matches the option in the client traffic.
2. Configure the default action—Specify the default processing action, which DHCPv6 relay uses for identified client traffic that does not satisfy any configured match criteria.

3. Create match filters and associate an action with each filter—Specify match criteria that filters the client traffic. The criteria can be an exact match or a partial match with the DHCPv6 option string in the client traffic. Associate a processing action with each match criteria.

Configuration

To configure group-level DHCPv6 relay agent selective processing based on DHCPv6 option information, perform these tasks:

- Configuring a DHCPv6 Relay Agent Named Interface Group To Selectively Process Client Traffic Based on DHCPv6 Option Strings on page 177
- Results on page 178

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level. The quick configuration assumes that the named interface group and the DHCP server groups have been previously configured.

```
set forwarding-options dhcp-relay dhcpv6 group groupv6-east-27
set forwarding-options dhcp-relay dhcpv6 relay-option option-number 15
set forwarding-options dhcp-relay dhcpv6 relay-option equals ascii triple-gold
  relay-server-group relayserver-triple-8
set forwarding-options dhcp-relay dhcpv6 relay-option equals ascii triple-silver
  relay-server-group relayserver-triple-23
set forwarding-options dhcp-relay dhcpv6 relay-option starts-with ascii single
  relay-server-group relayserver-1-aa
set forwarding-options dhcp-relay dhcpv6 relay-option default-action drop
```

Configuring a DHCPv6 Relay Agent Named Interface Group To Selectively Process Client Traffic Based on DHCPv6 Option Strings

Step-by-Step Procedure

This procedure assumes that you have previously created the named interface group and the DHCPv6 server groups. To configure DHCPv6 relay group-level selective processing:

1. Specify that you want to configure DHCPv6 relay agent support.

   ```
   [edit forwarding-options]
   user@host# edit dhcp-relay dhcpv6
   ```

2. Specify that you want to configure group-level DHCPv6 relay agent support.

   ```
   [edit forwarding-options dhcp-relay dhcpv6]
   user@host# edit group groupv6-east-27
   ```

3. Specify the DHCPv6 option number that DHCPv6 relay agent uses to identify incoming client traffic.

   ```
   [edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
   user@host# set relay-option option-number 15
   ```

4. Configure the default action, which DHCPv6 relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
user@host# set relay-option default-action relay-server-group relayserver-def-4
```

5. Configure an exact match condition and associated action that DHCPv6 relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
user@host# set relay-option equals ascii triple-gold relay-server-group
  relayserver-triple-8
```

6. Configure a second exact match condition and associated action that DHCPv6 relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
user@host# set relay-option equals ascii triple-silver relay-server-group
  relayserver-triple-23
```

7. Configure a partial match criteria and associated action that DHCPv6 relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
user@host# set relay-option starts-with ascii single relay-server-group
  relayserver-1-aa
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options dhcp]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dhcpv6 {
  group test-1 {
    relay-option {
      option-number 15;
      equals {
        ascii triple-gold {
          relay-server-group relayserver-triple-8;
        }
        ascii triple-silver {
          relay-server-group relayserver-triple-23;
        }
      }
      default-action {
        relay-server-group relayserver-def-4;
      }
      starts-with {
        ascii single {
          relay-server-group relayserver-1-aa;
        }
      }
    }
    interface ge-1/0/0.0 upto ge-1/1/0.0;
  }
  server-group {
    relayserver-1-aa;
    relayserver-triple-8;
```

```
        relayserver-triple-23;
        relayserver-def-4;
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To verify the status of DHCPv6 relay agent selective traffic processing, perform this task:

- Verifying the Status of DHCPv6 Relay Agent Selective Traffic Processing on page 179

Verifying the Status of DHCPv6 Relay Agent Selective Traffic Processing

Purpose Verify the DHCPv6 relay agent selective traffic processing status.

Action Display statistics for DHCPv6 relay agent.

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total                       0

Messages received:
    DHCPV6_DECLINE              0
    DHCPV6_SOLICIT              10
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE              0
    DHCPV6_REQUEST              10
    DHCPV6_CONFIRM              0
    DHCPV6_RENEW                0
    DHCPV6_REBIND               0
    DHCPV6_RELAY_REPL           0

Messages sent:
    DHCPV6_ADVERTISE            0
    DHCPV6_REPLY                0
    DHCPV6_RECONFIGURE          0
    DHCPV6_RELAY_FORW           0

Packets forwarded:
    Total                       4
    FWD REQUEST                 2
    FWD REPLY                   2
```

Meaning The **Packets forwarded** field in the **show dhcpv6 relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCPv6 relay agent has forwarded, as well as a breakdown for the number of **FWD REQUEST** and **FWD REPLY** packets forwarded.

Related Documentation

- *Extended DHCP Relay Agent Overview*
- *DHCPv6 Relay Agent Overview*
- *DHCP Options and Selective Traffic Processing Overview*

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*
- *Grouping Interfaces with Common DHCP Configurations*
- *Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings*
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 171

CHAPTER 9

Configuration Statements

[edit access domain] Hierarchy Level

```
access {
  domain {
    delimiter [delimiter-character];
    map domain-map-name {
      aaa-logical-system logical-system-name {
        aaa-routing-instance routing-instance-name;
      }
      aaa-routing-instance routing-instance-name;
      access-profile profile-name;
      address-pool pool-name;
      dynamic-profile profile-name;
      padn destination-address {
        mask destination-mask;
        metric route-metric;
      }
      strip-domain;
      target-logical-system logical-system-name {
        target-routing-instance routing-instance-name;
      }
      target-routing-instance routing-instance-name;
      tunnel-profile profile-name;
      tunnel-switch-profile profile-name;
    }
    parse-direction (left-to-right | right-to-left);
  }
}
```

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

[edit access profile] Hierarchy Level

```
access {
  profile profile-name {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      coa-immediate-update;
      coa-no-override service-class-attribute;
      duplication;
      immediate-update;
      order [ accounting-method ];
      statistics (time | volume-time);
      update-interval minutes;
      wait-for-acct-on-ack;
    }
    authentication-order [ authentication-methods ];
    authorization-order jsrc;
    client client-name {
      ...
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system–routing-instance;
          output-filter;
        }
      }
      authentication-server [ ip-address ];
      options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
        }
        client-accounting-algorithm (detail | round-robin);
        client-authentication-algorithm(detail | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
          exclude-adapter;
```

```
            exclude-sub-interface;
          }
          nas-identifier identifier-value;
          nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
              adapter-width width;
              port-width width:
              slot-width width;
              vci-width width:
              vpi-width width;
            }
          }
          nas-port-id-delimiter delimiter-character;
          nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
          }
          nas-port-type {
            ethernet {
              port-type;
            }
          }
          revert-interval interval;
          vlan-nas-port-stacked-format;
        }
      }
      radius-server server-address {
        accounting-port port-number;
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        max-outstanding-requests value;
        source-address source-address;
        timeout seconds;
      }
      service {
        accounting-order (activation-protocol | radius);
      }
      session-options {
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
  }
```

Related Documentation

- AAA Service Framework Overview on page 3

[edit interfaces radius-options] Hierarchy Level

```
interfaces interface-name {
  radius-options {
    nas-port-options nas-port-options-name {
      nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked;
        stacked-vlan-width width;
        vci-width width:
        vlan-width width;
        vpi-width width;
      }
      nas-port-type port-type;
      stacked-vlan-ranges (any | low-outer-tag–high-outer-tag),any;
      vlan-ranges (any | low-tag–high-tag);
    }
  }
}
```

Related Documentation

- RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 12
- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135

[edit system services subscriber-management] Hierarchy Level

```
system {
  services {
    subscriber-management {
      enforce-strict-scale-limit-license;
      gres-route-flush-delay;
      maintain-subscriber {
        interface-delete;
      }
      traceoptions {
        file <filename> <files number> <match regular-expression > <size
          maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
      }
    }
  }
}
```

Related Documentation

- *Subscriber Binding Retention During Interface Delete Events*
- *Configuring the Router to Strictly Enforce the Subscriber Scaling License*

- *Delaying Removal of Access Routes and Access-Internal Routes After Graceful Routing Engine Switchover*

aaa-logical-system (Domain Map)

Syntax

```
aaa-logical-system logical-system-name {
    aaa-routing-instance routing-instance-name;
}
```

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a non-default logical system in which the **authd** daemon sends AAA requests for the domain map.

NOTE: Subscriber management is supported in the default logical system only. The **aaa-logical-system** statement is for future extensions of subscriber management and is not supported in current Junos OS releases.

Default Default logical system for the subscriber.

Options ***logical-system-name***—Name of the logical system.

The remaining statement is explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying an AAA Logical System/Routing Instance in a Domain Map on page 156

aaa-routing-instance (Domain Map)

Syntax aaa-routing-instance *routing-instance-name*;

Hierarchy Level [edit access domain map *domain-map-name*],
[edit access domain map *domain-map-name* aaa-logical-system *logical-system-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a non-default routing instance in which the **authd** daemon sends AAA requests for the domain map.

Default Default routing instance for the subscriber.

Options ***routing-instance-name***—Name of the routing instance.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Specifying an AAA Logical System/Routing Instance in a Domain Map on page 156

access-loop-id-local

Syntax access-loop-id-local;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 13.1.

Description Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

access-profile (Domain Map)

Syntax access-profile *profile-name*;

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Access profile that defines the AAA services and options for subscribers associated with the domain map.

Options ***profile-name***—Name of access profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Specifying an Access Profile in a Domain Map on page 154

access-profile-name (Duplicate Accounting)

Syntax access-profile-name [*profile-name*];

Hierarchy Level [edit access profile *profile-name* accounting duplication-vrf]

Release Information Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Specify up to five access profiles, all in the same nondefault VRF (LS:RI combination), each of which lists one or more RADIUS accounting servers to which duplication accounting information is sent.

Options ***profile-name***—Name of an access profile that lists RADIUS accounting servers for duplicate reporting.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Understanding RADIUS Accounting Duplicate Reporting on page 21
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

accounting (Access Profile)

Syntax

```
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  address-change-immediate-update;
  coa-immediate-update;
  coa-no-override service-class-attribute;
  duplication;
  duplication-vrf {
    access-profile-name profile-name;
    vrf-name vrf-name;
  }
  immediate-update;
  order [ accounting-method ];
  statistics (time | volume-time);
  update-interval minutes;
  wait-for-acct-on-ack;
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Configuring Per-Subscriber Session Accounting on page 110
- Understanding RADIUS Accounting Duplicate Reporting on page 21

accounting-backup-options (Access Profile)

Syntax

```
accounting-backup-options {
  max-pending-accounting-stops number;
  max-withhold-time hold-time;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 13.1.

Description Configure options for backing up RADIUS accounting stop requests when all RADIUS accounting servers in the profile are offline.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- Configuring Back-up Options for RADIUS Accounting on page 115

accounting-port

Syntax accounting-port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the port number on which to contact the accounting server.

Options ***port-number***—Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- *Configuring RADIUS Authentication for L2TP*

accounting-server

Syntax accounting-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

Options ***ip-address***—IP version 4 (IPv4) address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

accounting-session-id-format

Syntax accounting-session-id-format (decimal | description);

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the format the router or switch uses to identify the accounting session.

Default **decimal**

Options **decimal**—Use the decimal format.

description—Use the generic format, in the form: **jnpr** *interface-specifier*:*subscriber-session-id*.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

accounting-stop-on-access-deny

Syntax accounting-stop-on-access-deny;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when the AAA server refuses a client request for access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

accounting-stop-on-failure

Syntax accounting-stop-on-failure;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

address-pool (Domain Map)

Syntax address-pool *pool-name*;

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the address pool used to assign addresses to subscribers associated with the domain map.

Options ***pool-name***—Name of address pool.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Specifying an Address Pool in a Domain Map on page 155

attributes

Syntax
```
attributes {
  exclude {
    ...
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system-routing-instance;
    output-filter;
  }
}
```

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify how the router or switch processes RADIUS attributes.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 129

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
none option introduced in Junos OS Release 11.2.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default password

Options *authentication-methods*

- **none**—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.

NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring CHAP Authentication with RADIUS*
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 109
- *Configuring Access Profiles for L2TP or PPP Parameters*

authentication-server

Syntax authentication-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options ***ip-address***—IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

calling-station-id-delimiter (Subscriber Management)

Syntax calling-station-id-delimiter *delimiter-character*;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 13.1.

Description Specify the character that the router uses as a separator between the concatenated values in the Calling-Station-ID (RADIUS IETF attribute 31) string. The router uses the delimiter when you configure more than one value in the **calling-station-id-format** statement.

Default The hash (**#**) character.

Options ***delimiter-character***—Character to use for the delimiter. You must enclose the delimiter character in quotation marks (“ ”).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring a Calling-Station-ID with Additional Attributes on page 127

calling-station-id-format (Subscriber Management)

Syntax

```
calling-station-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  nas-identifier;
}
```

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 13.1.

Description Specify the information that the router includes in the Calling-Station-ID (RADIUS IETF attribute 31) that is passed to the RADIUS server during authentication and accounting. You can include one or more optional values in any combination.

Default The router displays the Calling-Station-ID set by the client.

Options

agent-circuit-id—Include the agent circuit identifier (ACI) string, which uniquely identifies the subscriber's access node and the digital subscriber line (DSL) on the access node. The ACI string is stored in either the DHCP option 82 field of DHCP messages (for DHCP traffic), or in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE PADI and PADR control packets (for PPPoE traffic).

agent-remote-id—Include the agent remote identifier (ARI) string, which identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The ARI string is stored in either the DHCP option 82 field of DHCP messages (for DHCP traffic), or in the DSL Forum Agent-Remote-ID VSA [26-2] of PPPoE PADI and PADR control packets (for PPPoE traffic).

interface-description—Include the interface description.

nas-identifier—Include the NAS-identifier (RADIUS IETF attribute 32), which specifies the name of the NAS that orginated the authentication or accounting request.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring a Calling-Station-ID with Additional Attributes on page 127

client-accounting-algorithm

Syntax client-accounting-algorithm (direct | round-robin);

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the access method the router uses to access RADIUS accounting servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring RADIUS Server Options for Subscriber Access on page 118

client-authentication-algorithm

Syntax client-authentication-algorithm (direct | round-robin);

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the access method the router uses to access RADIUS authentication servers.

Default direct

Options **direct**—Use the direct method.

round-robin—Use the round-robin method.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring RADIUS Server Options for Subscriber Access on page 118

client-idle-timeout

Syntax client-idle-timeout *minutes*;

Hierarchy Level [edit access profile *profile-name* session-options]

Release Information Statement introduced in Junos OS Release 8.5.

Description (J Series, MX Series, and SRX Series devices) Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user.

Default The timeout is not configured.

Options ***minutes***—Number of minutes of idle time that elapse before the session is terminated.
Range: 10 through 1440 minutes

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- Understanding Session Options for Subscriber Access on page 27
- Configuring Subscriber Session Options on page 152
- Removing Inactive Dynamic Subscriber VLANs on page 29

client-session-timeout

Syntax client-session-timeout *minutes*;

Hierarchy Level [edit access profile *profile-name* session-options]

Release Information Statement introduced in Junos OS Release 8.5.

Description (J Series, MX Series, and SRX Series devices) Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout).

Default The timeout is not configured.

Options ***minutes***—Number of minutes after which user sessions are terminated.
Range: 1 through 527040 minutes

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- Understanding Session Options for Subscriber Access on page 27
- Configuring Subscriber Session Options on page 152

coa-dynamic-variable-validation

Syntax coa-dynamic-variable-validation;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 12.1.

Description Specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

Default If you do not configure this statement, the router does not apply any incorrect variable updates but does make any other changes to the client profile dynamic variables, and then responds with an ACK message.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- RADIUS Server Options for Subscriber Access on page 5
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

coa-immediate-update

Syntax coa-immediate-update;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 10.0.

Description Configure the router to send an Acct-Update message to the RADIUS accounting server immediately following a CoA operation.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring Per-Subscriber Session Accounting on page 110

coa-no-override service-class-attribute

Syntax coa-no-override service-class-attribute;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify that, after a CoA action that changes the RADIUS Class attribute, accounting reports for the subscriber's service sessions continue to use the original Class attribute that was assigned when the service sessions were created. The new Class attribute value is used in accounting reports for the subscriber session only.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring Per-Subscriber Session Accounting on page 110

database-replication (Subscriber Session Database)

Syntax
```
database-replication {
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 9.3.

Description Define operations for subscriber management session database replication processes.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

delimiter (Domain Map)

Syntax delimiter [*delimiter-character*];

Hierarchy Level [edit access domain]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the characters that the router uses to separate usernames from domain names.

Default The @ character.

Options ***delimiter-character***—One or more characters used as delimiters. You can specify a maximum of eight delimiters. You cannot use the semicolon (;) as a delimiter. Do not include spaces between characters.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying Domain Name Delimiters on page 159
- Configuring Domain Name Usage for Domain Maps on page 159

domain (Domain Map)

Syntax

```
domain {
  delimiter [delimiter-character];
  map domain-map-name {
    aaa-logical-system logical-system-name {
      aaa-routing-instance routing-instance-name;
    }
    aaa-routing-instance routing-instance-name;
    access-profile profile-name;
    address-pool pool-name;
    dynamic-profile profile-name;
    padn destination-address {
      mask destination-mask;
      metric route-metric;
    }
    strip-domain;
    target-logical-system logical-system-name {
      target-routing-instance routing-instance-name;
    }
    target-routing-instance routing-instance-name;
    tunnel-profile profile-name;
    tunnel-switch-profile profile-name;
  }
  parse-direction (left-to-right | right-to-left);
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring a Domain Map on page 153

domain-name-server (Routing Instances and Access Profiles)

Syntax domain-name-server *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is lower in preference than one configured with the domain-name-server-inet statement.

Options ***dns-address***—IPv4 address of the DNS name server.

Required Privilege Level admin—To view this statement in the configuration
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring DNS Name Server Addresses for Subscriber Management on page 150
- DNS Name Server Address Overview on page 26

domain-name-server-inet (Routing Instances and Access Profiles)

Syntax domain-name-server-inet *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement.

Options ***dns-address***—IPv4 address of the DNS name server.

Required Privilege Level admin—To view this statement in the configuration
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring DNS Name Server Addresses for Subscriber Management on page 150
- DNS Name Server Address Overview on page 26

domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax domain-name-server-inet6 *dns-address*;

Hierarchy Level [edit access],
[edit access profile]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the **[edit access]** hierarchy level or for an access profile at the **[edit access profile *profile-name*]** hierarchy level. You can configure more than one address by including the statement multiple times.

Options ***dns-address***—IPv6 address of the DNS name server.

Required Privilege Level admin—To view this statement in the configuration
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring DNS Name Server Addresses for Subscriber Management on page 150
- DNS Name Server Address Overview on page 26

duplication (Access Profile)

Syntax duplication;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 11.4.

Description Configure the router to send accounting reports to both the RADIUS accounting server configured in the access profile for the wholesaler and the RADIUS accounting server configured in the access profile for the retailer.

Default The router sends accounting reports to the accounting servers that are in the context in which the subscriber is authenticated.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Understanding RADIUS Accounting Duplicate Reporting on page 21

duplication-vrf (Duplicate Accounting)

Syntax

```
duplication-vrf {
  access-profile-name profile-name;
  vrf-name vrf-name;
}
```

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Configure the router to send duplicate accounting information to the RADIUS accounting servers defined in up to five access profiles all in the same nondefault VRF (LS:RI combination).

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Understanding RADIUS Accounting Duplicate Reporting on page 21
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

dynamic-profile (Domain Map)

Syntax dynamic-profile *profile-name*;

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Dynamic profile that is used for subscriber sessions associated with the domain map.

Options ***profile-name***—Name of dynamic profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying a Dynamic Profile in a Domain Map on page 156

ethernet-port-type-virtual

Syntax ethernet-port-type-virtual;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of **ethernet** in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of **virtual**.

NOTE: This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

exclude (RADIUS)

Syntax

```
exclude {
    acc-aggr-cir-id-asc [ access-request | accounting-start | accounting-stop ];
    acc-aggr-cir-id-bin [ access-request | accounting-start | accounting-stop ];
    acc-loop-cir-id [ access-request | accounting-start | accounting-stop ];
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off | accounting-stop
      ];
    accounting-terminate-cause [ accounting-off ];
    act-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    act-data-rate-up [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    act-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    att-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    att-data-rate-up [ access-request | accounting-start | accounting-stop ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    cos-shaping-rate [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    dhcp-options [ access-request | accounting-start | accounting-stop ];
    downstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop
      ];
    dsl-forum-attributes [ access-request | accounting-start | accounting-stop ];
    dsl-line-state [ access-request | accounting-start | accounting-stop ];
    dsl-type [ access-request | accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
      ];
    filter-id [ accounting-start | accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    max-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    max-data-rate-up [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
    max-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
    min-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-data-rate-up [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-dn [ access-request | accounting-start | accounting-stop ];
    min-lp-data-rate-up [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
      accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
```

```
    upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
}
```

Hierarchy Level [edit access profile *profile-name* radius attributes]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **downstream-calculated-qos-rate**, **dsl-forum-attributes**, and **upstream-calculated-qos-rate** introduced in Junos OS Release 11.4.
Options **cos-shaping-rate** and **filter-id** introduced in Junos OS Release 13.2.

Description Configure the router or switch to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute, Juniper Networks (vendor ID 4874) VSA number and name, or DSL Forum (vendor ID 3561) VSA number and name.

- **acc-aggr-cir-id-asc**—Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **acc-aggr-cir-id-bin**—Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
- **acc-loop-cir-id**—Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause.
- **act-data-rate-dn**—Juniper Networks VSA 26-114, Act-Data-Rate-Dn
- **act-data-rate-up**—Juniper Networks VSA 26-113, Act-Data-Rate-Up
- **act-interlv-delay-dn**—Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn
- **act-interlv-delay-up**—Juniper Networks VSA 26-124, Act-Interlv-Delay-Up
- **att-data-rate-dn**—Juniper Networks VSA 26-118, Att-Data-Rate-Dn
- **att-data-rate-up**—Juniper Networks VSA 26-117, Att-Data-Rate-Up
- **called-station-id**—RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
- **class**—RADIUS attribute 25, Class.
- **cos-shaping-rate**—Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **dhcp-gi-address**—Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-mac-address**—Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Juniper Networks VSA 26-55, DHCP-Options.
- **downstream-calculated-qos-rate**—Juniper Networks VSA 26-141
- **dsl-forum-attributes**—DSL Forum VSA (vendor ID 3561) as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- **dsl-line-state**—Juniper Networks VSA 26-127, DSL-Line-State
- **dsl-type**—Juniper Networks VSA 26-128, DSL-Type
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
- **filter-id**—RADIUS attribute 11, Filter-Id.
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper Networks VSA 26-42, Acct-Input-Gigapackets.

- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper Networks VSA 26-53, Interface-Desc.
- **max-data-rate-dn**—Juniper Networks VSA 26-120, Max-Data-Rate-Dn
- **max-data-rate-up**—Juniper Networks VSA 26-119, Max-Data-Rate-Up
- **max-interlv-delay-dn**—Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn
- **max-interlv-delay-up**—Juniper Networks VSA 26-123, Max-Interlv-Delay-Up
- **min-data-rate-dn**—Juniper Networks VSA 26-116, Min-Data-Rate-Dn
- **min-data-rate-up**—Juniper Networks VSA 26-115, Min-Data-Rate-Up
- **min-lp-data-rate-dn**—Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn
- **min-lp-data-rate-up**—Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier.
- **nas-port**—RADIUS attribute 5, NAS-Port.
- **nas-port-id**—RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Juniper Networks VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper Networks VSA 25-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **upstream-calculated-qos-rate**—Juniper Networks VSA 26-142

RADIUS message type

- **access-request**—RADIUS Access-Accept messages.
- **accounting-off**—RADIUS Accounting-Off messages.
- **accounting-on**—RADIUS Accounting-On messages.
- **accounting-start**—RADIUS Accounting-Start messages.
- **accounting-stop**—RADIUS Accounting-Stop messages.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access on page 116

ignore

Syntax

```
ignore {
  framed-ip-netmask;
  input-filter;
  logical-system-routing-instance;
  output-filter;
}
```

Hierarchy Level [edit access profile *profile-name* radius attributes]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.

Options

framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).

input-filter—Ignore Ingress-Policy-Name (VSA 26-10).

logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).

output-filter—Ignore Egress-Policy-Name (VSA 26-11).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access on page 116

immediate-update

Syntax

```
immediate-update;
```

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the router or switch to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring Per-Subscriber Session Accounting on page 110

interface-description-format

Syntax

```
interface-description-format {
  exclude-adapter;
  exclude-sub-interface;
}
```

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **exclude-adapter** and **exclude-sub-interface** introduced in Junos OS Release 10.4.

Description Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.

Options

exclude-adapter—Exclude the adapter from the interface description.

exclude-sub-interface—Exclude the subinterface from the interface description.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- RADIUS Server Options for Subscriber Access on page 5

map (Domain Map)

Syntax

```
map domain-map-name {
  aaa-logical-system logical-system-name {
    aaa-routing-instance routing-instance-name;
  }
  aaa-routing-instance routing-instance-name;
  access-profile profile-name;
  address-pool pool-name;
  dynamic-profile profile-name;
  padn destination-address {
    mask destination-mask;
    metric route-metric;
  }
  strip-domain;
  target-logical-system logical-system-name {
    target-routing-instance routing-instance-name;
  }
  target-routing-instance routing-instance-name;
  tunnel-profile profile-name;
  tunnel-switch-profile profile-name;
}
```

Hierarchy Level [edit access domain]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the domain map to use to map options and parameters to subscriber sessions based on the subscriber domain.

Options *domain-map-name*—Name of the domain map. The name is the same as the subscriber domain to which it will apply. For example, for the username **user1@xyz.com**, the domain map name is **xyz.com**.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring a Domain Map on page 153

mask (Domain Map)

Syntax mask *destination-mask*;

Hierarchy Level [edit access domain map *domain-map-name* padn *destination-address*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure the IP mask of the destination used in the PADN parameters for a domain map.

Options ***destination-mask***—Subnet mask of the destination.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring PADN Parameters for a Domain Map on page 162

max-outstanding-requests

Syntax max-outstanding-requests *requests*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-server *server-address*]

Release Information Statement introduced in Junos OS Release 11.4.

Description (M120, M320, MX Series routers) Configure the maximum number of outstanding requests for this RADIUS server. An increase in this value is immediate while a decrease is more gradual if the current number of outstanding requests exceeds the new value.

Options ***requests***—Maximum number of outstanding requests for this RADIUS server.

Range: 0 through 2000 outstanding requests per server

Default: 1000 outstanding requests per server

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring RADIUS Server Options for Subscriber Access on page 118
- show network-access aaa statistics on page 289
- clear network-access aaa statistics on page 272

max-pending-accounting-stops (Access Profile)

Syntax max-pending-accounting-stops *number*;

Hierarchy Level [edit access accounting-backup-options]

Release Information Statement introduced in Junos OS Release 13.1.

Description Set the maximum number of pending accounting stop requests that the router backs up while all the RADIUS accounting servers in the profile are offline.

Options **number**—Number of stops to hold.
Range: 1 through 168,000
Default: 168,000

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- Configuring Back-up Options for RADIUS Accounting on page 115

max-withhold-time (Access Profile)

Syntax max-withhold-time *hold-time*;

Hierarchy Level [edit access accounting-backup-options]

Release Information Statement introduced in Junos OS Release 13.1.

Description Set the timer that determines how long the router holds pending accounting stop requests. Any remaining accounting stop messages are flushed when the timer expires, even if the accounting server is again online.

Options ***hold-time***—Number of minutes.
Range: 1 through 1440
Default: 60

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- Configuring Back-up Options for RADIUS Accounting on page 115

metric (Domain Map)

Syntax metric *route-metric*;

Hierarchy Level [edit access domain map *domain-map-name* padn *destination-address*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure the route metric PADN parameter for a domain map.

Options ***route-metric***—Value assigned to the route.
Range: 0 through 255

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring PADN Parameters for a Domain Map on page 162

nas-identifier

Syntax nas-identifier *identifier-value*;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

Options ***identifier-value***—String to use for authentication and accounting requests.
Range: 1 through 64 characters

Required Privilege Level admin—To view this statement in the configuration.
admin–control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

nas-port-extended-format (Access Profile)

Syntax

```
nas-port-extended-format {
  adapter-width width;
  ae-width width;
  port-width width;
  slot-width width;
  stacked;
  stacked-vlan-width width;
  vlan-width width;
  atm {
    adapter-width width;
    port-width width:
    slot-width width;
    vci-width width:
    vpi-width width;
  }
}
```

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Option **ae-width** introduced in Junos OS Release 12.1.
Option **stacked** introduced in Junos OS Release 12.3.
Option **atm** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Option **atm** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description In an access profile, configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. You can use the same access profile to configure the NAS-Port extended format for Ethernet subscribers and ATM subscribers.

Options

adapter-width *width*—Number of bits in the adapter field.

ae-width *width*—Number of bits in the aggregated Ethernet identifier field.

port-width *width*—Number of bits in the port field.

slot-width *width*—Number of bits in the slot field.

stacked—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vlan-width *width*—Number of bits in the VLAN ID field.

atm—Configure the NAS-Port extended format for ATM subscribers; options include:

- **adapter-width *width***—Number of bits in the adapter field.

- **port-width *width***—Number of bits in the port field.
- **slot-width *width***—Number of bits in the slot field.
- **vci-width *width***—Number of bits in the ATM virtual circuit identifier (VCI) field.
- **vpi-width *width***—Number of bits in the ATM virtual path identifier (VPI) field.

NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

nas-port-extended-format (Interfaces)

Syntax

```
nas-port-extended-format {
  adapter-width width;
  ae-width width;
  port-width width;
  slot-width width;
  stacked;
  stacked-vlan-width width;
  vci-width width:
  vlan-width width;
  vpi-width width;
}
```

Hierarchy Level [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]

Release Information Statement introduced in Junos OS Release 12.3.
Options **vci-width** and **vpi-width** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Options **vci-width** and **vpi-width** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

Options

adapter-width *width*—Number of bits in the adapter field.

ae-width *width*—Number of bits in the aggregated Ethernet identifier field.

port-width *width*—Number of bits in the port field.

slot-width *width*—Number of bits in the slot field.

stacked—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vci-width *width*—Number of bits in the ATM virtual circuit identifier (VCI) field.

vlan-width *width*—Number of bits in the VLAN ID field.

vpi-width *width*—Number of bits in the ATM virtual path identifier (VPI) field.

NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

nas-port-id-delimiter (Subscriber Management)

Syntax
nas-port-id-delimiter *delimiter-character*;

Hierarchy Level
[edit access profile *profile-name* radius options]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the **nas-port-id-format** statement.

Default
The hash (**#**) character.

Options
delimiter-character—Character used for the delimiter.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring a NAS-Port-ID with Additional Options on page 125

nas-port-id-format (Subscriber Management)

Syntax

```
nas-port-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  nas-identifier;
}
```

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that it is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

Default The router includes the interface description.

Options

agent-circuit-id—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.

agent-remote-id—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.

interface-description—Include the interface description.

nas-identifier—Include the NAS identifier value (RADIUS attribute 32).

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring a NAS-Port-ID with Additional Options on page 125

nas-port-options (RADIUS Options)

Syntax

```
nas-port-options nas-port-options-name {
  nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked;
    stacked-vlan-width width;
    vci-width width:
    vlan-width width;
    vpi-width width;
  }
  nas-port-type port-type;
  stacked-vlan-ranges (any | low-outer-tag–high-outer-tag),any;
  vlan-ranges (any | low-tag–high-tag);
}
```

Hierarchy Level [edit interfaces *interface-name* radius-options]

Release Information Statement introduced in Junos OS Release 12.3.

Description Create a NAS-Port options definition to configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis. Each NAS-Port options definition includes the NAS-Port extended format, the NAS-Port-Type, and either the VLAN range of subscribers or the S-VLAN range of subscribers to which the definition applies.

NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options ***nas-port-options-name***—Name of the NAS-Port options definition.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

nas-port-type (Subscriber Management)

Syntax

```
nas-port-type {
  ethernet {
    port-type;
  }
}
```

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).

NOTE: This statement is ignored if the ethernet-port-type-virtual statement is included in the same access profile.

Default The router uses a port type of **ethernet**.

Options ***port-type***—One of the following port types:

- *value*—A value from 0-65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**— Asymmetric DSL, discrete multitone (DMT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **idsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120
- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL
- **sync**—Synchronous

- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV
- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring RADIUS Server Parameters for Subscriber Access on page 116

nas-port-type (RADIUS Options)

Syntax nas-port-type *port-type*;

Hierarchy Level [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the port type used to authenticate subscribers. The router includes the port type in the NAS-Port-Type (61) RADIUS IETF attribute.

Default If you do not include the **nas-port-type** statement at the **[edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]** hierarchy level, the global value configured for nas-port-type at the **[edit access profile *profile-name* radius options]** hierarchy level takes effect.

Options ***port-type***—One of the following port types:

- *value*—A value from 0 through 65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**— Asymmetric DSL, discrete mutilating (DOT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **idsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120
- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL
- **sync**—Synchronous
- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV

- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

options (Access Profile)

Syntax

```
options {
  accounting-session-id-format (decimal | description);
  calling-station-id-delimiter delimiter-character;
  calling-station-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  coa-dynamic-variable-validation;
  ethernet-port-type-virtual;
  access-loop-id-local;
  interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
  }
  ip-address-change-notify message;
  juniper-dsl-attributes;
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
      adapter-width width;
      port-width width:
      slot-width width;
      vci-width width:
      vpi-width width;
    }
  }
  nas-port-id-delimiter delimiter-character;
  nas-port-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  nas-port-type {
    ethernet {
      port-type;
    }
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
```

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the options used by RADIUS authentication and accounting servers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- RADIUS Server Options for Subscriber Access on page 5

order

Syntax order [*accounting-method*];

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Set the order in which the Junos OS tries different accounting methods for client activity. When a client logs in, the software tries the accounting methods in the specified order.

Options ***accounting-method***—One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last. The only valid value is **radius** for RADIUS accounting.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

padn (Domain Map)

Syntax

```
padn destination-address {
  mask destination-mask;
  metric route-metric;
}
```

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure PADN parameters for a domain map.

Options ***destination-address***—IP address of the destination.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring PADN Parameters for a Domain Map on page 162

parse-direction (Domain Map)

Syntax parse-direction (left-to-right | right-to-left);

Hierarchy Level [edit access domain]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the direction in which the router searches for the domain name in a username.

Default right-to-left

Options **left-to-right**—The router searches starting at the left-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.

right-to-left—The router searches starting at the right-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying the Parsing Direction for Domain Names on page 160
- Configuring Domain Name Usage for Domain Maps on page 159

port

Syntax port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the port number on which to contact the RADIUS server.

Options ***port-number***—Port number on which to contact the RADIUS server.

Default: 1812 (as specified in RFC 2865)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

profile (Access)

Syntax

```
profile profile-name {
  accounting {
    address-change-immediate-update
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    duplication-vrf {
      access-profile-name profile-name;
      vrf-name vrf-name;
    }
    immediate-update;
    order [ accounting-method ];
    send-acct-status-on-config-change;
    statistics (time | volume-time);
    update-interval minutes;
    wait-for-acct-on-ack;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      aaa-access-profile profile-name;
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
```

```
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
      user-group-profile profile-name;
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      authentication-server [ ip-address ];
      options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
          exclude-adapter;
          exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
          adapter-width width;
          ae-width width;
          port-width width;
          slot-width width;
          stacked-vlan-width width;
          vlan-width width;
          atm {
            adapter-width width;
            port-width width:
            slot-width width;
            vci-width width:
            vpi-width width;
          }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
```

```
        }
        nas-port-type {
          ethernet {
            port-type;
          }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
      }
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system:routing-instance;
          output-filter;
        }
      }
    }
    radius-server server-address {
      accounting-port port-number;
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      max-outstanding-requests value;
      source-address source-address;
      timeout seconds;
    }
    service {
      accounting-order (activation-protocol | radius);
    }
    session-options {
      client-group [ group-names ];
      client-idle-timeout minutes;
      client-session-timeoutminutes;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring the PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Configuring Service Accounting with JSRC*
- AAA Service Framework Overview on page 3
- show network-access aaa statistics on page 289
- clear network-access aaa statistics on page 272

radius (Access Profile)

Syntax

```
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        ip-address-change-notify message;
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
                adapter-width width;
                port-width width:
                slot-width width;
                vci-width width:
                vpi-width width;
            }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
```

```
        agent-remote-id;
        interface-description;
        nas-identifier;
      }
      nas-port-type {
        ethernet {
          port-type;
        }
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- RADIUS Server Options for Subscriber Access on page 5

radius-options (Edit Access)

Syntax

```
radius-options {
  revert-interval seconds;
  request-rate rate;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 8.3.

Description Configure RADIUS options.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

radius-options (Interfaces)

Syntax

```
radius-options {
  nas-port-options nas-port-options-name {
    nas-port-extended-format {
      adapter-width width;
      ae-width width;
      port-width width;
      slot-width width;
      stacked;
      stacked-vlan-width width;
      vci-width width:
      vlan-width width;
      vpi-width width;
    }
    nas-port-type port-type;
    stacked-vlan-ranges (any | low-outer-tag–high-outer-tag),any;
    vlan-ranges (any | low-tag–high-tag);
  }
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure RADIUS options to set the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

radius-server

Syntax

```
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry attempts;
  routing-instance routing-instance-name;
  secret password;
  max-outstanding-requests value;
  source-address source-address;
  timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring RADIUS Authentication for L2TP*
- *Configuring the PPP Authentication Protocol*
- *Configuring RADIUS Authentication*
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*
- show network-access aaa statistics on page 289
- clear network-access aaa statistics on page 272

report-interface-descriptions (Edit Access)

Syntax report-interface-descriptions;

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 13.1.

Description Enable storing and reporting of interface descriptions through RADIUS. To disable storing and reporting of interface descriptions, configure the **[edit access profile *profile-name* radius attributes exclude]** statement to exclude the interface description attribute. The description can contain letters, numbers, and hyphens (-), and can be up to 64 characters long.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- exclude on page 207
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Subscriber Access Interface Description Storage and Reporting Through RADIUS Overview on page 121

request network-access aaa replay pending-accounting-stops

Syntax request network-access aaa replay pending-accounting-stops

Release Information Command introduced in Junos OS Release 13.1.

Description Force the router to attempt contact with the accounting sever immediately, rather than allowing it to wait until the periodic interval has expired.

Options This command has no options.

Required Privilege Level view

Related Documentation
- Forcing the Router to Contact the Accounting Server Immediately on page 116
- show accounting pending-accounting-stops on page 275

List of Sample Output request network-access aaa replay pending-accounting-stops on page 240

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request network-access aaa replay pending-accounting-stops

```
user@host> request network-access aaa replay pending-accounting-stops
replay started
```

request-rate

Syntax request-rate *rate*;

Hierarchy Level [edit access radius-options]

Release Information Statement introduced in Junos OS Release 11.4.

Description (M120, M320, and MX Series routers) Configure the number of requests the router can send per second to all configured RADIUS servers collectively. By limiting the flow of requests from the router to the RADIUS servers, you can prevent the RADIUS servers from being flooded with requests.

Options *rate*—Number of requests per second.

Range: 500 through 4000 requests per second

Default: 500 requests per second

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Router or Switch Interaction with RADIUS Servers on page 108

retry

Syntax retry *attempts*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.

Options ***attempts***—Number of times that the router is allowed to attempt to contact a RADIUS server.

Range: 1 through 10

Default: 3

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- timeout on page 252

revert-interval

Syntax revert-interval *interval*;

Hierarchy Level [edit access profile *profile-name* radius options],
[edit access radius-options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.

Options ***interval***—Amount of time to wait.

Range: 0 through 604800 seconds

Default: 60 seconds

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

routing-instance

Syntax routing-instance *routing-instance-name*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the routing instance used to send RADIUS packets to the RADIUS server.

Options ***routing-instance-name***—Routing instance name.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring the PPP Authentication Protocol*
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

secret

Syntax secret *password*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-disconnect *client-address*],
[edit access radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

Options ***password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- *Configuring the RADIUS Disconnect Server for L2TP*
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*

send-acct-status-on-config-change (Access Profile)

Syntax send-acct-status-on-config-change

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 13.1.

Description Configure the router's authd process to send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring Per-Subscriber Session Accounting on page 110

session-options

Syntax

```
session-options {
  client-group [ group-names ];
  client-idle-timeout minutes;
  client-session-timeoutminutes;
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description (J Series, MX Series, and SRX Series devices) Define options that control a user's session after successful authentication.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- Understanding Session Options for Subscriber Access on page 27
- Configuring Subscriber Session Options on page 152

source-address

Syntax source-address *source-address*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

Options ***source-address***—Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*

stacked-vlan-ranges (RADIUS Options)

Syntax stacked-vlan-ranges (any | *low-outer-tag–high-outer-tag*),any;

Hierarchy Level [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure the stacked VLAN (S-VLAN) range of subscribers to which the named NAS-Port options definition applies.

NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options **any**—Entire S-VLAN range representing all S-VLAN IDs. The inner tag (S-VLAN ID) of the S-VLAN range must be configured as **any** to represent all inner VLAN ID tags.

low-outer-tag—Outer VLAN ID tag representing the lower limit of the S-VLAN range.
Range: 1 through 4094

high-outer-tag—Outer VLAN ID tag representing the upper limit of the S-VLAN range.
Range: 1 through 4094

NOTE: To specify a single outer VLAN ID tag, set ***low-outer-tag*** and ***high-outer-tag*** to the same value.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

statistics (Access Profile)

Syntax statistics (time | volume-time);

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Option **volume-time** introduced in Junos OS Release 9.4.

Description Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.

Options **time**—Collect uptime statistics only.

volume-time—Collect both volume and uptime statistics. This option is not available for Mobile IP.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- *Mobile IP Home Agent Elements and Behavior*
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

strip-domain (Domain Map)

Syntax strip-domain;

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Remove the domain name from the username before continuing with any AAA services specified in a domain map.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Enabling Domain Name Stripping on page 161
- Configuring Domain Name Usage for Domain Maps on page 159

target-logical-system (Domain Map)

Syntax

```
target-logical-system logical-system-name {
    target-routing-instance routing-instance-name;
}
```

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a non-default logical system and optionally a non-default routing instance for the subscriber's interface in a domain map.

You use the target-routing-instance statement at the **[edit access domain map *domain-map-name*]** hierarchy level to configure a non-default routing instance for the default logical system.

NOTE: Subscriber management is supported in the default logical system only. The target-logical-system statement is for future extensions of subscriber management and is not supported in current Junos OS releases.

Default Default logical system for the subscriber..

Options ***logical-system-name***—Name of the logical system.

The remaining statement is explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying a Target Logical System/Routing Instance in a Domain Map on page 158

target-routing-instance (Domain Map)

Syntax target-routing-instance *routing-instance-name*;

Hierarchy Level [edit access domain map *domain-map-name*],
[edit access domain map *domain-map-name* target-logical-system *logical-system-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a non-default routing instance for the target logical system for the subscriber's interface in a domain map.

- When configured at the **[edit access domain map *domain-map-name*]** hierarchy level, this statement configures the routing instance used with the default target logical system.
- When configured at the **[edit access domain map *domain-map-name* target-logical-system *logical-system-name*]** hierarchy level, this statement configures the routing instance used with the specified non-default target logical system.

Default Default routing instance for the subscriber.

Options ***routing-instance-name***—Name of the routing instance.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Specifying a Target Logical System/Routing Instance in a Domain Map on page 158

terminate-code

Syntax

```
terminate-code {
  (aaa (deny | shutdown) | dhcp | l2tp | ppp) term-reason radius term-cause;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 11.4.

Description Customize mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute.

Options

aaa—Defines AAA as the protocol type, and specifies either the **deny** or **shutdown** action to perform with the specified terminate reason.

dhcp—Defines DHCP as the protocol type associated with the specified terminate reason.

l2tp—Defines L2TP as the protocol type associated with the specified terminate reason.

ppp—Defines PPP as the protocol type associated with the specified terminate reason.

term-reason—Terminate reason for the specified protocol type.

term-cause—Standards-based RADIUS Acct-Terminate-Cause code that identifies the terminate reason.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Custom Terminate Reason Mappings on page 100
- AAA Terminate Reasons on page 74
- DHCP Terminate Reasons on page 75
- L2TP Terminate Reasons on page 76
- PPP Terminate Reasons on page 92

timeout (RADIUS)

Syntax timeout *seconds*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.

Options ***seconds***—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 108
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*

traceoptions (Subscriber Session Database Replication)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit system services database-replication]

Release Information Statement introduced in Junos OS Release 9.3.

Description Define tracing operations for subscriber management session database replication processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **database**—Trace database events.
- **general**—Trace general flow.
- **mirror**—Trace mirroring events.
- **replication**—Trace database replication events.
- **server**—Trace server events.
- **session-db**—Trace session database interactions.
- **ui**—Trace user interface events.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to

indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

traceoptions (Subscriber Management)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit system services subscriber-management]

Release Information Statement introduced in Junos OS Release 11.1.

Description Define tracing operations for subscriber management interface processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **database**—Trace database events.
- **general**—Trace general events.
- **issu**—Trace unified ISSU events.
- **server**—Trace server events.
- **session-db**—Trace session database interactions.
- **ui**—Trace user interface events.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

tunnel-profile (Domain Map)

Syntax tunnel-profile *profile-name*;

Hierarchy Level [edit access domain map *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Tunnel profile that provides definitions for tunnels associated with the domain map.

Options ***profile-name***—Name of tunnel profile.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Specifying a Tunnel Profile in a Domain Map on page 161
- *Configuring a Tunnel Profile for Subscriber Access*

update-interval

Syntax update-interval *minutes*;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Enable interim accounting updates and configure the amount of time that the router or switch waits before sending a new accounting update.

Default No updates

Options ***minutes***—Amount of time between updates, in minutes. All values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.

Range: 10 through 1440 minutes

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

vlan-nas-port-stacked-format

Syntax vlan-nas-port-stacked-format;

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Options for Subscriber Access on page 118
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

vlan-ranges (RADIUS Options)

Syntax vlan-ranges (any | *low-tag–high-tag*);

Hierarchy Level [edit interfaces *interface-name* radius-options nas-port-options *nas-port-options-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure the VLAN range of subscribers to which the named NAS-Port options definition applies.

NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options **any**—Entire VLAN range representing all VLAN IDs.

low-tag—VLAN ID tag representing the lower limit of the VLAN range.
Range: 1 through 4094

high-tag—VLAN ID tag representing the upper limit of the VLAN range.
Range: 1 through 4094

NOTE: To specify a single VLAN ID, set ***low-tag*** and ***high-tag*** to the same value.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 135
- Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 14

vrf-name (Duplicate Accounting)

Syntax vrf-name *vrf-name*;

Hierarchy Level [edit access profile *profile-name* accounting duplication-vrf]

Release Information Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Specify a nondefault VRF (LS:RI combination) to which duplicate accounting information is sent. Up to five access profiles can be defined in this VRF; the profiles point to the RADIUS accounting servers that receive the accounting information.

Options ***vrf-name***—Name of a nondefault VRF to receive duplicate accounting reports.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Understanding RADIUS Accounting Duplicate Reporting on page 21
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 109

wait-for-acct-on-ack (Access Profile)

Syntax wait-for-acct-on-ack;

Hierarchy Level [edit access profile *profile-name* accounting]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure the router's **authd** process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access on page 116
- Configuring Per-Subscriber Session Accounting on page 110

PART 3

Administration

CHAPTER 10

Verifying and Managing Configurations

Verifying and Managing Subscriber AAA Information

Purpose View or clear subscriber access statistics and information.

Action

- To display subscriber AAA statistics:

  user@host> show network-access aaa statistics

  user@host> show network-access aaa statistics authentication

- To display RADIUS server status and information:

  user@host> show network-access aaa radius-servers

- To display subscriber access AAA information:

  user@host> show network-access aaa subscribers

- To display subscriber session information:

  user@host> show network-access aaa subscribers session-id ***session-id***

- To clear subscriber access statistics and to log out specific subscribers:

  user@host> clear network-access aaa subscriber

- To clear AAA accounting statistics:

  user@host> clear network-access aaa statistics **accounting**

- To clear AAA address-assignment statistics for a client:

  user@host> clear network-access aaa statistics **address-assignment client**

- To clear AAA address-assignment pool statistics:

  user@host> clear network-access aaa statistics **address-assignment pool** ***pool-name***

- To clear AAA authentication statistics:

  user@host> clear network-access aaa statistics **authentication**

Related Documentation

- *Junos OS Operational Mode Commands*

Monitoring Pending RADIUS Accounting Stop Messages

Purpose Display information about RADIUS accounting stop messages that are being withheld due to an inability to contact the RADIUS accounting server.

Action When you want to know whether the number of pending accounting-stop messages is nearing the maximum, you can display a simple count of pending requests:

```
user@host> show network-access aaa statistics pending-accounting-stops
Pending accounting stops: 10,000
```

You can use other commands to display more information about the accounting messages. The next example displays information for all services in the accounting session for the user, vjshah29@example.com. Although this example shows only one user, this command actually displays the information for all subscribers for whom accounting is being backed up.

```
user@host> show accounting pending-accounting-stops detail
Type: pppoe
Username: vjshah29@example.com
AAA Logical system/Routing instance: default:default
Access-profile: ce-ppp-profile
Session ID: 84
Accounting Session ID: 84
IP Address: 192.168.0.25
IPv6 Prefix: 2010:9999:18::/48
Authentication State: AuthAcctStopAckWait
Accounting State: Acc-Stop-Stats-Pending
Service name: cos-service
  Service State: SvcInactive
  Session ID: 94
  Session uptime: 00:08:02
  Accounting status: on/time
  Service accounting session ID: 84:94-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service
  Service State: SvcInactive
  Session ID: 93
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:93-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service6
  Service State: SvcInactive
  Session ID: 95
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:95-1352294677
```

```
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
```

You can display summary information for all users with a particular access profile. In the following example, only a single user, vjshah29@example.com, has the specified access profile, ce-ppp-profile:

```
user@host> show accounting pending-accounting-stops ce-ppp-profile

Type:         Username:               Session ID:     Service ID:       Service
  pppoe        vjshah29@example.com       84
  pppoe        vjshah29@example.com       84              94               cos-service
  pppoe        vjshah29@example.com       84              93               filter-service
  pppoe        vjshah29@example.com       84              95               filter-service6
```

You can also display summary information for all subscribers that have accounting-stop messages pending, regardless of access profile. The next example displays information for two users. Because the subscriber larry@example.com is not shown in the previous example, he must have a different access profile than vjshah29@example.com, even though he has received the same services.

```
user@host> show accounting pending-accounting-stops terse

 Type:         Username:                  Session ID:     Service ID:       Service
  pppoe        vjshah29@example.com          84
  pppoe        vjshah29@example.com          84              94               cos-service
  pppoe        vjshah29@example.com          84              93               filter-service
  pppoe        vjshah29@example.com          84              95               filter-service6
  pppoe        larry@example.com             85
  pppoe        larry@example.com             85              94               cos-service
  pppoe        larry@example.com             85              93               filter-service
  pppoe        larry@example.com             85              95               filter-service6
```

Related Documentation

- Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 22
- Configuring Back-up Options for RADIUS Accounting on page 115

Monitoring DHCP Options Configured on RADIUS Servers

Purpose View information for DHCP options that are centrally configured on a RADIUS server and that are distributed using Juniper Networks VSA 26-55 (DHCP-Options).

Action To display information for opaque DHCP options:

```
user@host> show subscribers detail
Type: DHCP
IP Address: 192.168.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-prof-23
MAC Address: 00:10:95:00:00:98
State: Active
```

Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2011-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c

Meaning

```
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
```

The DHCP options output provides the following information:

- The **len** field is the total number of hex values in the message.
- The hex values specify the type, length, and value (TLV) of DHCP options, and are converted to decimal to identify the DHCP options, as defined in RFC 2132.

The number of hex values that make up a particular DHCP option varies, depending on the length of the option. For example, the first DHCP option specified in the output includes three sets of hex values (**35 01 01**). The first hex value (**35**) identifies the option type, the second value (**01**) indicates the length of the value entry, which is this case is one set of hex values. The third hex value (**01**) specifies the value for the DHCP option.

In the second DHCP option specification (**39 02 02 40**), the hex value **39** is the type, and the length of **02** specifies that two sets of hex entries make up the value for the option. Therefore, this option specification uses four sets of hex entries; one for the type (**39**), one to specify the length (**02**), and two for the option value (**02 40**).

The third DHCP option is specified by the hex values **3d 07 01 00 10 94 00 00 08**. The hex value **3d** is the type, followed by the length (**07**), which specifies that the next seven sets of hex entries make up the value for the option. Therefore, this option specification uses a total of nine sets of hex entries; one for the type (**3d**), one to specify the length (**07**), and seven for the value of the DHCP option (**01 00 10 94 00 00 08**).

Table 29 on page 267 describes the first two options in more detail.

Table 29: DHCP Options Description

Option	Type	Length	Value
35 01 01	35 = decimal 53 (Code 53 in RFC 2132 is the DHCP Message Type option)	01 = the length of the option is one set of hex values (the next set in the list)	01 = value of the message type that is described in RFC 2132. The code 01 specifies a message type of DHCPDISCOVER.
39 02 02 40	39 = decimal 57 (Code 57 is the Maximum DHCP Message Size option)	02 = the length of the option is two sets of hex values (the next two sets in the list)	0240 = converted to a length of 576 octets

Related Documentation

- Centrally Configured Opaque DHCP Options on page 15
- show subscribers on page 304

Verifying and Managing the RADIUS Dynamic-Request Feature

Purpose Display RADIUS dynamic request statistics and information.

Action

- To display RADIUS dynamic request statistics:

  user@host>show network-access aaa statistics **dynamic-requests**

Related Documentation

- *Junos OS Operational Mode Commands*

Verifying and Managing Domain Map Configuration

Purpose Display information related to a domain map.

Action

- To display statistics for the domain map:

  user@host> show network-access domain-map

- To display domain map information for a specific subscriber session:

  user@host> show network-access aaa subscribers session-id

Related Documentation

- Domain Mapping Overview on page 103
- Configuring a Domain Map on page 153

Testing a Subscriber AAA Configuration

Purpose Display the AAA attributes that subscriber management assigns to the subscriber during login.

The following example tests the AAA configuration for a PPP subscriber. You can use the test aaa dhcp user command to perform a similar test for DHCP subscribers and the test aaa authd-lite user command to test authd-lite subscribers.

NOTE: The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

Action `user@host>test aaa ppp user thomastank password 00N15&`

```
Authentication Grant
************User Attributes***********
     User Name -                          thomastank
     Client IP Address -                  192.168.1.1
     Client IP Netmask -                  255.255.0.0
     Virtual Router Name -                default
     Reply Message -                      NULL
     Primary DNS IP Address -             0.0.0.0
     Secondary DNS IP Address -           0.0.0.0
     Primary WINS IP Address -            0.0.0.0
     Secondary WINS IP Address -          0.0.0.0
     Framed Pool -                        addr_pool2
     Session Timeout -                    0
     Idle Timeout -                       0
     Service Type -                       0
     Client Ipv6 Address -                ::
     Client Ipv6 Mask -                   null
     Framed Ipv6 Prefix -                 ::/0
     Framed Ipv6 Pool -                   not-set
     Nas Ipv6 Address -                   ::
     NDRA Ipv6 Prefix -                   not-set
     Login Ipv6 Host -                    ::
     Framed Interface Id: -               0:0:0:0
     Delegated Ipv6 Prefix -              ::/0
     Delegated Ipv6 Pool -                not-set
     User Password -                      00N15&
     CHAP Password -                      NULL
     NAS Ip Address -                     0.0.0.0
     Agent Remote Id -                    not-set
     NAS Port -                           0
     NAS Port Type -                      5
Client Session Activate request sent
Client Session Activated
     Filter Id -                          not set
     Framed MTU -                         (null)
     Framed Route -                       not set
     Ingress Policy Name -                not set
     Egress Policy Name -                 not set
     IGMP -                               disabled
     Redirect VR Name -                   default
     Service Bundle -                     Null
     Framed Ip Route Tag -                not set
     LI Action -                          0
     LI Intercpet Id -                    0
     Med Ipaddress -                      0.0.0.0
     Med Port Number -                    0
     Ignore DF Bit -                      disabled
     IGMP Access Group Name -             not set
     IGMP Access Source Group Name -      not set
     MLD Access Group Name -              not set
     MLD Access Source Group Name -       not set
     IGMP Version -                       IGMP Version not set
     MLD Version -                        MLD Version not set
     IGMP Immediate Leave -               disabled
     MLD Immediate Leave -                disabled
     IPv6 Ingress Policy Name -           not set
     IPv6 Egress Policy Name -            not set
     Cos Parameter Type -                 not-set
```

```
        Cos  Scheduler Parameter Type -          not-set
        Acct Session ID-                         8
        Acct Interim Interval -                  0
        Acct Type -                              0
        Ingress Statistics                       disabled
        Egress Statistics                        disabled
****Pausing 10 seconds before disconnecting the test user*********
Logging out subscriber
Test complete. Exiting
```

If you specify the DSL Forum Agent-Remote-Id (VSA 26-2), the output includes the specified value:

```
user@host>test aaa ppp user thomastank agent-remote-id "(202)555–1212"

    Authentication Grant
    ************User Attributes***********
        User Name -                          thomastank
        Client IP Address -                  192.168.1.1
        Client IP Netmask -                  255.255.0.0
        ...
        NAS Ip Address -                     0.0.0.0
        Agent Remote Id -                    (202)555-1212
        ...
```

If you do not specify the VSA, then the Agent-Remote-Id value is shown as **not-set**.

Related Documentation

- AAA Configuration Testing and Troubleshooting on page 29

CHAPTER 11

Monitoring Commands

clear network-access aaa statistics

Syntax

clear network-access aaa statistics
<accounting>
<address-assignment (client | pool *pool-name*)>
<authentication>
<dynamic-requests>
<radius>
<re-authentication>
<terminate-code>

Release Information

Command introduced in Junos OS Release 10.0.
Option **radius** introduced in Junos OS Release 11.4
Option **terminate-code** introduced in Junos OS Release 11.4.

Description

Clear AAA statistics.

Options

accounting—(Optional) Clear AAA accounting statistics.

address-assignment client—(Optional) Clear AAA address-assignment statistics for the client.

address-assignment pool *pool-name*—(Optional) Clear AAA address-assignment pool statistics.

authentication—(Optional) Clear AAA authentication statistics.

dynamic-requests—(Optional) Clear AAA dynamic-request statistics.

radius—(Optional) Clears the values in the **Peak** and **Exceeded** columns only.

re-authentication—(Optional) Clear AAA reauthentication statistics.

terminate-code—(Optional) Clear AAA termination code statistics.

Required Privilege Level

maintenance

Related Documentation

- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output

clear network-access aaa statistics accounting on page 272
clear network-access aaa statistics address-assignment pool on page 273
clear network-access aaa statistics radius on page 273

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access aaa statistics accounting

```
user@host> clear network-access aaa statistics accounting
```

clear network-access aaa statistics address-assignment pool

```
user@host> clear network-access aaa statistics address-assignment pool isp_1
```

clear network-access aaa statistics radius

```
user@host> clear network-access aaa statistics radius
```

clear network-access aaa subscriber

Syntax clear network-access aaa subscriber
<statistics username *username*>
<username *username*>

Release Information Command introduced in Junos OS Release 9.1.

Description Clear AAA subscriber statistics and log out subscribers.

Options **statistics username *username***—Clear AAA subscriber statistics and log out the subscriber.

username *username*—Log out the AAA subscriber.

Required Privilege Level maintenance

Related Documentation
- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output
clear network-access aaa subscriber statistics username on page 274
clear network-access aaa subscriber username on page 274

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access aaa subscriber statistics username

```
user@host> clear network-access aaa subscriber statistics username dsmith@isp5555.com
```

clear network-access aaa subscriber username

```
user@host> clear network-access aaa subscriber username dsmith@isp5555.com
```

show accounting pending-accounting-stops

Syntax **show accounting pending-accounting-stops**
<detail | terse>
<*profile-name*>

Release Information Command introduced in Junos OS Release 13.1.

Description Display all statistics for all pending accounting stop requests, including both service and session requests.

Options **none**—Display information for all access profiles.

detail | terse—(Optional) Display the specified level of output.

profile-name—(Optional) Particular access profile for which you want to display accounting stop statistics.

Required Privilege Level view

Related Documentation
- request network-access aaa replay pending-accounting-stops on page 240
- show network-access aaa statistics pending-accounting-stops on page 295

List of Sample Output
show accounting pending-accounting-stops detail on page 277
show accounting pending-accounting-stops (Specific Profile) on page 277
show accounting pending-accounting-stops terse on page 277

Output Fields Table 30 on page 275 lists the output fields for the **show accounting pending-accounting-stops** command. Output fields are listed in the approximate order in which they appear.

Table 30: show accounting pending-accounting-stops Output Fields

Field Name	Field Description	Level of Output
Type	Type of client.	All levels
Username	Name of the user logged in to the session.	All levels
Logical system/Routing instance	Logical system and routing instance used for the session.	**detail** none
Access-profile	Access profile used for AAA services for the session.	**detail** none
Session ID	ID of the subscriber session; generated when the subscriber logs in. In the **Service name** block, this is the ID of the service session.	All levels

Table 30: show accounting pending-accounting-stops Output Fields *(continued)*

Field Name	Field Description	Level of Output
Accounting Session ID	ID of the accounting session (RADIUS attribute 44). The ID appears in decimal or description format, as specified by the **accounting-session-id-format** statement.	**detail** none
IP Address	IP address of the subscriber.	**detail** none
IPv6 Prefix	IPv6 address of the subscriber.	**detail** none
Authentication State	State of the subscriber authentication session: **AuthInit, AuthStart, AuthChallenge, AuthRedirect, AuthClntRespWait, AuthAcctVolStatsAckWait, AuthAcctStopAckWait, AuthServCreateRespWait, AuthLogoutStart, AuthStateActive, AuthClntLogoutRespWait, AuthProfileUpdateWait, AuthProvisionRespWait, AuthProvisionServiceCreationWait**	**detail** none
Accounting State	State of the subscriber accounting session: **Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd**	**detail** none
Service name	Name of the attached service or policy.	**detail** none
Service State	State of the service provided in the subscriber session.	**detail** none
Session uptime	How long the session has been up, in *HH:MM:SS*.	**detail** none
Accounting status	Status of the accounting configuration for the service, **on** or **off**, and the type of accounting, **time** or **volume+time**. Configured in RADIUS Service-Statistics VSA [26-69].	**detail** none
Service accounting session ID	ID of the service accounting session; RADIUS Acct-Session-Id attribute (44). The ID appears in decimal or description format, as specified by the **accounting-session-id-format** statement.	**detail** none
Service accounting state	State of the service accounting session: **Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd**	**detail** none
Accounting interim interval	Amount of time between interim accounting updates for this service, in seconds; RADIUS Service-Interim-Acct-Interval VSA [26-140] or Diameter Acct-Interim-Interval AVP (85).	**detail** none
Subscriber ID	ID of the subscriber; generated when the subscriber logs in.	**detail** none
Service ID	ID of the subscriber service.	All levels
Service	Name of the attached service or policy.	**terse**

Sample Output

show accounting pending-accounting-stops detail

```
user@host> show accounting pending-accounting-stops detail
Type: pppoe
Username: vjshah29@example.com
AAA Logical system/Routing instance: default:default
Access-profile: ce-ppp-profile
Session ID: 84
Accounting Session ID: 84
IP Address: 192.168.0.25
IPv6 Prefix: 2010:9999:18::/48
Authentication State: AuthAcctStopAckWait
Accounting State: Acc-Stop-Stats-Pending
Service name: cos-service
  Service State: SvcInactive
  Session ID: 94
  Session uptime: 00:08:02
  Accounting status: on/time
  Service accounting session ID: 84:94-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service
  Service State: SvcInactive
  Session ID: 93
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:93-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service6
  Service State: SvcInactive
  Session ID: 95
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:95-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
```

show accounting pending-accounting-stops (Specific Profile)

```
user@host> show accounting pending-accounting-stops ce-ppp-profile

Type:         Username:               Session ID:     Service ID:       Service
  pppoe        vjshah29@example.com       84
  pppoe        vjshah29@example.com       84              94               cos-service
  pppoe        vjshah29@example.com       84              93               filter-service
  pppoe        vjshah29@example.com       84              95               filter-service6
```

show accounting pending-accounting-stops terse

```
user@host> show accounting pending-accounting-stops terse

 Type:         Username:                  Session ID:     Service ID:       Service
  pppoe        vjshah29@example.com          84
  pppoe        vjshah29@example.com          84              94               cos-service
  pppoe        vjshah29@example.com          84              93               filter-service
  pppoe        vjshah29@example.com          84              95               filter-service6
  pppoe        larry@example.com             85
  pppoe        larry@example.com             85              94               cos-service
```

```
pppoe        larry@example.com          85          93          filter-service
pppoe        larry@example.com          85          95          filter-service6
```

show database-replication statistics

Syntax show database-replication statistics

Release Information Command introduced in Junos OS Release 9.3.

Description Display statistics regarding the replication of the subscriber management session database.

Options This command has no options.

Required Privilege Level view

Related Documentation
- show database-replication summary on page 281

List of Sample Output show database-replication statistics on page 279

Output Fields Table 31 on page 279 lists the output fields for the **show database-replication statistics** command. Output fields are listed in the approximate order in which they appear.

Table 31: show database-replication statistics Output Fields

Field Name	Field Description
General	Number of dropped connections and the maximum buffer count.
Message Received	Total size of messages received and the number of received messages that have been processed.
Message Sent	Total size of messages sent and the number of sent messages that have been processed.
Message Queue	Number of messages in the queue and the maximum size of the queue.

Sample Output

show database-replication statistics

```
user@host> show database-replication statistics

General:
    Dropped connections         0
    Max buffer count            0
Message received:
    Size (bytes)                0
    Processed                   0
Message sent:
    Size (bytes)                0
    Processed                   0
Message queue:
```

```
Queue full                0
Max queue size            0
```

show database-replication summary

Syntax show database-replication summary

Release Information Command introduced in Junos OS Release 9.3.

Description Display summary information regarding database replication for the subscriber management session database.

Options This command has no options.

Required Privilege Level view

Related Documentation
- show database-replication statistics on page 279

List of Sample Output show database-replication summary on page 282

Output Fields Table 32 on page 281 lists the output fields for the **show database-replication summary** command. Output fields are listed in the approximate order in which they appear.

Table 32: show database-replication summary Output Fields

Field Name	Field Description
Graceful Restart	State of graceful Routing Engine switchover (GRES): • **Enabled** • **Disabled**
Mastership	State of the Routing Engine: • **Master** • **Standby**
Connection	State of the connection: • **Up** • **Down**
Database	State of the subscriber management database: • **Available** • **Unavailable** • **Synchronized**
Message Queue	State of the message queue: • **Full** • **Init** • **Not Ready** • **Ready**

Sample Output

show database-replication summary

```
user@host> show database-replication summary
General:
    Graceful Restart     Enabled
    Mastership           Standby
    Connection           Up
    Database             Available
    Message Queue        Ready
```

show network-access aaa accounting

Syntax **show network-access aaa accounting**

Release Information Command introduced in Junos OS Release 12.3.

Description Display the state of the RADIUS Acct-On response sent from the RADIUS server.

Required Privilege Level view

Related Documentation
- RADIUS Acct-On and Acct-Off Messages on page 25

List of Sample Output show network-access aaa accounting on page 283

Output Fields Table 33 on page 283 lists the output fields for the **show network-access aaa accounting** command. Output fields are listed in the approximate order in which they appear.

Table 33: show network-access aaa accounting Output Fields

Field Name	Field Description
Profile	Name of the profile associated with the RADIUS server. A RADIUS server can be associated with more than one profile.
Logical System	Logical system associated with the access profile.
Routing Instance	Routing instance associated with the access profile.
Acct-On-Response	Status of the RADIUS Acct-On response. • ACK—ACK response for the Acct-On message is received from the RADIUS server. • ERROR—An error condition has occurred. • NONE— No Acct-On message is sent. • PENDING—Acct-On message is sent to RADIUS server, but no response has been received yet.

Sample Output

show network-access aaa accounting

```
user@host> show network-access aaa accounting
Profile        Logical System   Routing Instance   Acct-On-Response
ppp-profile    default          default            ACK
l2tp-profile   default          l2tp_RI            PENDING
```

show network-access aaa radius-servers

Syntax **show network-access aaa radius-servers**
<detail>

Release Information Command introduced in Junos OS Release 12.1.

Description Display RADIUS server status and information.

Options **detail**—(Optional) Display detailed level of information.

Required Privilege Level view

Related Documentation
- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output
show network-access aaa radius-servers on page 287
show network-access aaa radius-servers on page 287
show network-access aaa radius-servers detail on page 288

Output Fields Table 34 on page 284 lists the output fields for the **show network-access aaa radius-servers** command. Output fields are listed in the approximate order in which they appear.

Table 34: show network-access aaa radius-servers Output Fields

Field Name	Field Description	Level of Output
Profile	Name of the profile associated with the RADIUS server. A RADIUS server can be associated with more than one profile.	All levels
Server address	IP address of the RADIUS server.	All levels
Authentication port	RADIUS server authentication port number.	All levels
Accounting port	RADIUS server accounting port number.	All levels

Table 34: show network-access aaa radius-servers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Status	RADIUS server status, **UP** (Alive), **UNREACHABLE**, or **DOWN** (DEAD). If status is **DOWN**, the Status field includes the number of seconds configured by the **revert-interval** statement. The router does not send request to servers in the **DOWN** state, but does send requests to servers with a status of either **UP** or **UNREACHABLE**. NOTE: After requests to a server or set of servers time out after 10 seconds, the status of the servers changes. The following guidelines apply to server status: • All servers cannot be marked as **DOWN**; instead, the unresponsive servers are marked as **UNREACHABLE**. For example, if only one RADIUS server is configured and that server is unresponsive, the server status is marked as **UNREACHABLE** rather than **DOWN**. • If at least one server has a status of **UP**, the status of all unresponsive servers is set to **DOWN** for the remainder of the configured revert-interval setting. • If no server has a status of **UP**, then the status of the unresponsive servers is set to **UNREACHABLE** for the remainder of the revert-interval setting or for 30 seconds, whichever is less. • The status of unresponsive servers is returned to **UP** from **DOWN** or **UNREACHABLE** at the end of the revert-interval setting (or the 30-second interval). • If no requests are sent to a server, the server's status is always **UP**.	All levels
RADIUS servers	Details for specific RADIUS server, identified by IP address.	Detail
Authentication requests	Number of authentication requests received by the authentication server.	Detail
Authentication rollover requests	Number of requests coming into the server as a result of the previous server timing out.	Detail
Authentication retransmissions	Number of retransmissions.	Detail
Accepts	Number of authentication requests accepted by the authentication server.	Detail
Rejects	Number of authentication requests rejected by the authentication server.	Detail

Table 34: show network-access aaa radius-servers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Challenges	Number of authentication requests challenged by the authentication server.	Detail
Authentication malformed responses	Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).	Detail
Authentication bad authenticators	Number of responses in which the authenticator is incorrect for the authentication request. This can occur if the RADIUS secrets for the client and server do not match.	Detail
Authentication requests pending	Number of authentication requests waiting for a response.	Detail
Authentication request timeouts	Number of times an authentication request to the server timed out.	Detail
Authentication unknown responses	Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.	Detail
Authentication packets dropped	Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request.	Detail
Accounting start requests	Number of accounting start requests received.	Detail
Accounting interim requests	Number of accounting interim requests received.	Detail
Accounting stop requests	Number of accounting stop requests received.	Detail
Accounting rollover requests	Number of requests coming into the server as a result of the previous server timing out.	Detail
Accounting retransmissions	Number of retransmissions.	Detail
Accounting start responses	Number of accounting start responses sent by the server.	Detail
Accounting interim responses	Number of accounting interim responses sent by the server.	Detail
Accounting stop responses	Number of accounting stop responses sent by the server.	Detail

Table 34: show network-access aaa radius-servers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Accounting malformed responses	Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).	Detail
Accounting bad authenticators	Number of responses in which the authenticator is incorrect for the accounting request. This can occur if the RADIUS secrets for the client and server do not match.	Detail
Accounting requests pending	Number of accounting requests waiting for a response.	Detail
Accounting request timeouts	Number of accounting requests to the accounting server that timed out.	Detail
Accounting unknown responses	Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.	Detail
Accounting packets dropped	Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request.	Detail

Sample Output

show network-access aaa radius-servers

```
user@host> show network-access aaa radius-servers
Profile: xyz-profile1
    Server address: 192.168.30.188
      Authentication port: 1645
      Accounting port: 1646
      Status: UP
  Profile: xyz-profile2
    Server address: 192.168.30.190
      Authentication port: 1812
      Accounting port: 1813
      Status: DOWN ( 60 seconds )
```

show network-access aaa radius-servers

```
user@host> show network-access aaa radius-servers
Profile: xyz-profile3
    Server address: 192.168.30.188
      Authentication port: 1645
      Accounting port: 1646
      Status: UNREACHABLE
Profile: xyz-profile3
    Server address: 192.168.30.190
      Authentication port: 1812
      Accounting port: 1813
      Status: UNREACHABLE
```

show network-access aaa radius-servers detail

```
user@host> show network-access aaa radius-servers detail
Profile: xyz_profile5
    Server address: 192.168.30.188
      Authentication port: 1812
      Accounting port: 1813
      Status: UP

RADIUS Servers
  192.168.30.188
    Authentication requests: 7658
    Authentication rollover requests: 0
    Authentication retransmissions: 3600
    Accepts: 6458
    Rejects: 0
    Challenges: 0
    Authentication malformed responses: 0
    Authentication bad authenticators: 0
    Authentication requests pending: 0
    Authentication request timeouts: 4800
    Authentication unknown responses: 0
    Authentication packets dropped: 0
    Accounting start requests: 1
    Accounting interim requests: 1
    Accounting stop requests: 0
    Accounting rollover requests: 0
    Accounting retransmissions: 0
    Accounting start responses: 1
    Accounting interim responses: 1
    Accounting stop responses: 0
    Accounting malformed responses: 0
    Accounting bad authenticators: 0
    Accounting requests pending: 0
    Accounting request timeouts: 0
    Accounting unknown responses: 0
    Accounting packets dropped: 0
```

show network-access aaa statistics

Syntax

show network-access aaa statistics
<accounting>
<address-assignment (client | pool *pool-name*)>
<dynamic-requests>
<radius>

Release Information

Command introduced in Junos OS Release 9.1.
Option **address-assignment** introduced in Junos OS Release 10.0.
Option **radius** introduced in Junos OS Release 11.4.

Description

Display AAA accounting, address-assignment, dynamic request statistics, and RADIUS settings and statistics.

Options

accounting—(Optional) Display AAA accounting statistics.

address-assignment (client | pool *pool-name*)—(Optional) Display AAA address-assignment client and pool statistics.

dynamic-requests—(Optional) Display AAA dynamic requests.

radius— (Optional) Display RADIUS settings and statistics.

Required Privilege Level

view

Related Documentation

- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output

show network-access aaa statistics accounting on page 291
show network-access aaa statistics address-assignment client on page 291
show network-access aaa statistics address-assignment pool on page 291
show network-access aaa statistics dynamic-requests on page 291
show network-access aaa statistics radius on page 291

Output Fields

Table 35 on page 289 lists the output fields for the **show network-access aaa statistics** command. Output fields are listed in the approximate order in which they appear.

Table 35: show network-access aaa statistics Output Fields

Field Name	Field Description
Requests received	• Number of accounting requests generated by the AAA framework. • Number of dynamic requests received from the external server.
Accounting Response failures	Number of accounting requests not acknowledged (NAK) by the accounting server.
Accounting Response Success	Number of accounting requests acknowledged by the accounting server.

Table 35: show network-access aaa statistics Output Fields *(continued)*

Field Name	Field Description
Requests timedout	Number of accounting requests to the accounting server that timed out.
Client	Client type; for example, DHCP, Mobile IP, PPP.
Out of Memory	Number of times an address was not given to the client due to memory issues.
No Matches	Number of times there were no network matches for the pool.
Pool Name	Name of the address-assignment pool for this client.
Out of Addresses	Number of times there were no available addresses in the pool.
Address total	Number of addresses in the pool.
Addresses in use	Number of addresses in use.
Address Usage (percent)	Percentage of total addresses in use.
processed successfully	Number of dynamic requests processed successfully by the AAA framework.
errors during processing	Number of dynamic requests that resulted in processing errors by the AAA framework.
Link Name	Name of the secondary address-assignment pool to which the primary pool is linked.
Pool Usage	Percentage of allocated addresses in the specified address pool.
silently dropped	Number of dynamic requests dropped by the AAA framework due to multiple back-to-back or duplicate requests.
RADIUS Server	IP address of the RADIUS server to which the router is sending requests.
Profile	Name of the RADIUS profile associated with the RADIUS server. A RADIUS server can be associated with more than one RADIUS profile.
Configured	Configured maximum number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded. The range of values is 0 through 2000 outstanding requests. The default value is 1000.
Current	Current number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded.
Peak	Highest number of outstanding requests from the router to the RADIUS server for a specific profile at any point in time since the router was started or since the counter was last cleared. NOTE: If the value of this field is equal to the value of the **Configured** field, you may want to increase the value of the **Configured** field.

Table 35: show network-access aaa statistics Output Fields *(continued)*

Field Name	Field Description
Exceeded	Number of times that the router attempted to send requests to the RADIUS server in excess of the configured maximum value for a specific profile. NOTE: If the value of this field is nonzero, you may want to increase the value of the **Configured** field.

Sample Output

show network-access aaa statistics accounting

```
user@host> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 0
  Accounting Response failures: 0
  Accounting Response Success: 0
  Requests timedout: 0
```

show network-access aaa statistics address-assignment client

```
user@host> show network-access aaa statistics address-assignment client
Address-assignment statistics
 Client: jdhcpd
 Out of Memory: 0
 No Matches: 2
```

show network-access aaa statistics address-assignment pool

```
user@host> show network-access aaa statistics address-assignment pool isp_1
Address-assignment statistics
 Pool Name: isp_1
 Pool Name: (all pools in chain)
 Out of Memory: 0
 Out of Addresses: 9
 Address total: 47
 Addresses in use: 47
 Address Usage (percent): 100
```

show network-access aaa statistics dynamic-requests

```
user@host> show network-access aaa statistics dynamic-requests
requests received: 0
processed successfully: 0
errors during processing: 0
silently dropped: 0
```

show network-access aaa statistics radius

```
user@host> show network-access aaa statistics radius
Outstanding Requests
RADIUS Server     Profile      Configured   Current   Peak   Exceeded
172.28.32.239     prof1        1000         0         1000   14
                  prof2        500          17        432    0
171.27.82.211     myprof       200          0         200    27
12.1.11.254     pppoe-auth     111          0         1      0
```

show network-access aaa statistics authentication

Syntax **show network-access aaa statistics authentication <detail>**

Release Information Command introduced in Junos OS Release 9.1.
Option **detail** introduced in Junos OS Release 12.1.

Description Display AAA authentication statistics.

Options **detail**—(Optional) Displays detailed information about authentication.

Required Privilege Level view

Related Documentation
- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output
show network-access aaa statistics authentication on page 294
show network-access aaa statistics authentication detail on page 294

Output Fields Table 36 on page 292 lists the output fields for the **show network-access aaa statistics authentication** command. Output fields are listed in the approximate order in which they appear.

Table 36: show network-access aaa statistics authentication Output Fields

Field Name	Field Description	Level of Output
Requests received	Number of authentication requests received from clients.	All levels
Multistack requests	Number of authentication requests for dual-stack subscribers.	All levels
Accepts	Number of authentication requests accepted by the authentication server.	All levels
Rejects	Number of authentication requests rejected by the authentication server.	All levels
Challenges	Number of authentication requests challenged by the authentication server.	All levels
Requests timed out	Number of authentication requests that timed out.	All levels
RADIUS authentication failures	Number of RADIUS authentication requests that have failed.	Detail
Queue request deleted	Number of queue requests that have been deleted.	Detail

Table 36: show network-access aaa statistics authentication Output Fields *(continued)*

Field Name	Field Description	Level of Output
Malformed reply	Number of malformed replies received from the RADIUS authentication server.	Detail
No server configured	Number of authentication requests that failed because no authentication server is configured.	Detail
Access Profile configuration not found	Number of authentication requests that failed because no access profile is configured.	Detail
Unable to create client record	Number of times that the router is unable to create the client record for the authentication request.	Detail
Unable to create client request	Number of times that the router is unable to create the client request for the authentication request.	Detail
Unable to build authentication request	Number of times that the router is unable to build the authentication request.	Detail
No server found	Number of requests to the authentication server that have timed out; the server is then considered to be down.	Detail
Unable to create handle	Number of authentication requests that have failed because of an internal allocation failure.	Detail
Unable to queue request	Number of times the router was unable to queue the request to the authentication server.	Detail
Invalid credentials	Number of times the router did not have proper authorization to access the authentication server.	Detail
Malformed request	Number of times the router request to the authentication server is malformed.	Detail
License unavailable	Number of times the router did not have a license to access the authentication server.	Detail
Redirect requested	Number of authentication requests that have been redirected based on routing instance.	Detail
Internal failure	Number of internal failures.	Detail
Local authentication failures	Number of times local authentication failed.	Detail
LDAP lookup failures	Number of times the LDAP lookup operation failed.	Detail

Sample Output

show network-access aaa statistics authentication

```
user@host> show network-access aaa statistics authentication
Authentication module statistics
  Requests received: 2118
  Multistack requests: 0
  Accepts: 261
  Rejects: 975
  Challenges: 0
  Requests timed out: 882
```

show network-access aaa statistics authentication detail

```
user@host> show network-access aaa statistics authentication detail
Authentication module statistics
  Requests received: 2118
  Multistack requests: 0
  Accepts: 261
  Rejects: 975
    RADIUS authentication failures: 975
      Queue request deleted: 0
      Malformed reply: 0
      No server configured: 0
      Access Profile configuration not found: 0
      Unable to create client record: 0
      Unable to create client request: 0
      Unable to build authentication request: 0
      No server found: 975
      Unable to create handle: 0
      Unable to queue request: 0
      Invalid credentials: 0
      Malformed request: 0
      License unavailable: 0
      Redirect requested: 0
      Internal failure: 0
    Local authentication failures: 0
    LDAP lookup failures: 0
  Challenges: 0
  Requests timed out: 882
```

show network-access aaa statistics pending-accounting-stops

Syntax **show network-access aaa statistics pending-accounting-stops**

Release Information Command introduced in Junos OS Release 13.1.

Description Display the number of pending accounting stop requests.

Options This command has no options.

Required Privilege Level view

Related Documentation
- request network-access aaa replay pending-accounting-stops on page 240
- show accounting pending-accounting-stops on page 275

List of Sample Output show network-access aaa statistics pending-accounting-stops on page 295

Output Fields Table 37 on page 295 lists the output field for the **show network-access aaa statistics pending-accounting-stops** command.

Table 37: show network-access aaa statistics pending-accounting-stops Output Fields

Field Name	Field Description
Pending accounting stops	Total number of accounting stop messages queued.

Sample Output

show network-access aaa statistics pending-accounting-stops

```
user@host> show network-access aaa statistics pending-accounting-stops
Pending accounting stops: 10,000
```

show network-access aaa subscribers

Syntax

show network-access aaa subscribers
<logical-system *logical-system-name*>
<routing-instance *routing-instance-name*>
<statistics>
<username>

Release Information

Command introduced in Junos OS Release 9.1.

Description

Display subscriber-specific AAA statistics.

Options

logical-system *logical-system-name*—(Optional) List subscribers in the specific logical system.

routing-instance *routing-instance-name*—(Optional) List subscribers for the specific routing instance. If you do not specify a routing instance name, the default routing instance is assumed.

statistics—(Optional) Display statistics for the subscriber events.

username—(Optional) Display information for the specified subscriber.

Required Privilege Level

view

Related Documentation

- Verifying and Managing Subscriber AAA Information on page 263

List of Sample Output

show network-access aaa subscribers logical-system on page 297
show network-access aaa subscribers logical-system routing-instance on page 297
show network-access aaa subscribers statistics username on page 298
show network-access aaa subscribers username on page 298

Output Fields

Table 38 on page 296 lists the output fields for the **show network-access aaa subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 38: show network-access aaa subscribers Output Fields

Field Name	Field Description
Challenge requests	Number of authentication requests challenged by the authentication server for this subscriber.
Challenge responses	Number of challenge responses sent by the subscriber to the authentication server.
START sent successfully	Number of accounting start requests generated by the AAA framework for this subscriber.
START send failures	Number of accounting start requests that failed to make it to the accounting server for this subscriber.
START ack received	Number of accounting start requests acknowledged by the accounting server for this subscriber.

Table 38: show network-access aaa subscribers Output Fields *(continued)*

Field Name	Field Description
INTERIM sent successfully	Number of accounting interim requests generated by the AAA framework for this subscriber.
INTERIM send failures	Number of accounting interim requests that failed to make it to the accounting server for this subscriber.
INTERIM ack received	Number of accounting interim requests acknowledged by the accounting server for this subscriber.
Requests received	Number of reauthentication requests received by the authentication server.
Successful responses	Number of successful reauthentication requests granted by the authentication server.
Aborts handled	Number of reauthentication requests aborted by the authentication server.
Service name	Name of the subscriber service.
Creation requests	Number of requests to create the service.
Deletion requests	Number of requests to delete the service.
Request timeouts	Number of times the service request was timed out.
Client type	Type of client; for example, DHCP, Mobile IP, PPP.
Session-ID	ID of the subscriber session.
Session uptime	How long the session has been up, in *HH:MM:SS*.
Accounting	Status of accounting, and type of accounting if accounting is on.

Sample Output

show network-access aaa subscribers logical-system

```
user@host> show network-access aaa subscribers logical-system
Username            Client type    Logical system/Routing instance
cbenson@addr.net    ppp            default
00010e020304.1231   dhcp           isp-bos-metro-12:isp-cmbrg-12
conley@isp3.com     dhcp           default:isp-gtown-r3-00
0020df980102.2334   dhcp           isp-bos-metro-16:isp-cmbrg-12
```

show network-access aaa subscribers logical-system routing-instance

```
user@host> show network-access aaa subscribers logical-system isp-bos-metro-16
routing-instance isp-cmbrg-12-32
Username            Client type   Logical system/Routing instance
00010e020304.1231   dhcp          isp-bos-metro-12:isp-cmbrg-12
conley@isp3.com     dhcp          default:isp-gtown-r3-00
0020df980102.2334   dhcp          isp-bos-metro-16:isp-cmbrg-12
```

show network-access aaa subscribers statistics username

```
user@host> show network-access aaa subscribers statistics username 00010e020304.1231
Authentication statistics
   Challenge requests: 0
   Challenge responses: 0
 Accounting statistics
   START sent successfully: 1
   START send failures: 0
   START ack received: 1
   INTERIM sent successfully: 0
   INTERIM send failures: 0
   INTERIM ack received: 0
 Re-authentication statistics
   Requests received: 0
   Sucessfull responses: 0
   Aborts handled: 0
 Service statistics
   Service name: filter-serv
   Creation requests: 1
   Deletion requests: 0
   Request timeouts: 0
   Service name: filter-serv2
   Creation requests: 144
   Deletion requests: 0
   Request timeouts: 144
```

show network-access aaa subscribers username

```
user@host> show network-access aaa subscribers username fred@isp5.net
Logical system/Routing instance   Client type  Session-ID  Session uptime
Accounting
isp-bos-metro-16:isp-cmbrg-12     dhcp         7           01:12:56
on/volume
Service name       Service type      Quota          Accounting
I-Cast             volume            1200 Mbps      on/volume+time
Voip                                                on/volume
GamingBurst        time              6000 secs      on/volume
```

show network-access aaa subscribers session-id

Syntax **show network-access aaa subscribers session-id** *session-id* **<brief | detail>**

Release Information Command introduced in Junos OS Release 10.0.

Description Display information about the specified subscriber session.

Options ***session-id***—ID of the subscriber session.

brief | detail—(Optional) Display the specified level of information.

Required Privilege Level view

Related Documentation
- Verifying and Managing Subscriber AAA Information on page 263
- *Activating and Deactivating Subscriber Services Locally with the CLI*

List of Sample Output
show network-access aaa subscribers session-id brief on page 301
show network-access aaa subscribers session-id detail on page 301

Output Fields Table 39 on page 299 lists the output fields for the **show network-access aaa subscribers session-id** command. Output fields are listed in the approximate order in which they appear.

Table 39: show network-access aaa subscribers session-id Output Fields

Field Name	Field Description	Level of Output
Type and **Client type**	Type of client.	All levels
Accounting	Status of accounting, and type of accounting if accounting is on.	brief
Service type	Type of accounting: **volume**, **time**, **volume+time**, or **na**.	brief
Quota	Quota for service: volume (in Mbps) or time (seconds).	brief
Username	Name of the user logged in to the session.	detail
Stripped username	Username after the domain has been removed.	detail
Logical system/Routing instance and **AAA Logical system/Routing instance**	Name of the routing instance, logical system name, or both used for the session.	All levels

Table 39: show network-access aaa subscribers session-id Output Fields *(continued)*

Field Name	Field Description	Level of Output
Target Logical system/Routing instance	Logical system/routing instance to which the session is mapped.	detail
Access-profile	Access profile used for AAA services for the session.	detail
Session ID	ID of the subscriber session. The session ID value displayed under **Service name** is the service session ID.	detail
Accounting Session ID	ID of the accounting session (RADIUS attribute 44). The ID appears in decimal or description format, as specified by the **accounting-session-id-format** statement.	detail
Multi Accounting Session ID	Bundle ID for MLPPP sessions. Acct-Multi-Session-Id (RADIUS attribute 50) uses the value of the session database bundle session ID to enable RADIUS to link together multiple related sessions. The value of this field is zero when no MLPPP sessions exist.	detail
IP Address	IP address of the subscriber.	detail
Authentication State	State of the subscriber authentication session: **AuthInit, AuthStart, AuthChallenge, AuthRedirect, AuthClntRespWait, AuthAcctVolStatsAckWait, AuthAcctStopAckWait, AuthServCreateRespWait, AuthLogoutStart, AuthStateActive, AuthClntLogoutRespWait, AuthProfileUpdateWait, AuthProvisionRespWait, AuthProvisionServiceCreationWait**	detail
Gx-Plus Provisioning State	State of Gx-Plus provisioning: • ignored—Subscriber has no IPv4 address or NAS-Port-ID. • in-progress—Provisioning is in progress. • logout—Subscriber logout is in progress. • logout-done—Logout response has been received. • response-received—Provisioning response has been received.	detail
Accounting State	State of the subscriber accounting session: **Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd**	detail

Table 39: show network-access aaa subscribers session-id Output Fields *(continued)*

Field Name	Field Description	Level of Output
Provisioning-type	Provisioning type for this session: • gx-plus—Subscriber service uses Gx-Plus provisioning. • jsrc—Subscriber service uses JSRC provisioning. • none—Provisioning is not enabled.	detail
Service name	Name of the attached service or policy. • For JSRC-activated policies—displays the policy name.	All levels
Service State	State of the service provided in the subscriber session.	detail
Session uptime	How long the session has been up, in *HH:MM:SS*.	All levels
Accounting status	Status of the accounting configuration for the service, **on** or **off**, and the type of accounting, **time** or **volume+time**. Configured in RADIUS Service-Statistics VSA [26-69].	detail
Service accounting session ID	ID of the service accounting session; RADIUS Acct-Session-Id attribute (44). The ID appears in decimal or description format, as specified by the **accounting-session-id-format** statement.	detail
Service accounting state	State of the service accounting session: **Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd**	detail
Accounting interim interval	Amount of time between interim accounting updates for this service, in seconds; RADIUS Service-Interim-Acct-Interval VSA [26-140] or Diameter Acct-Interim-Interval AVP (85).	detail

Sample Output

show network-access aaa subscribers session-id brief

```
user@host> show network-access aaa subscribers session-id 6 brief
Logical system/Routing instance   Client type   Session uptime    Accounting
default:default                   dhcp          00:01:29          on/time
Service name              Service type   Quota          Accounting
filter-service            -na-           -na-           off
1337994190863204450       -na-           -na-           off
```

show network-access aaa subscribers session-id detail

```
user@host> show network-access aaa subscribers session-id 5 detail
```

```
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 5
Accounting Session ID: jnpr ge-1/0/0.101:1
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Gx-Plus Provisioning State: response-received
Accounting State: Acc-Interim-Sent
Provisioning-type: jsrc
Service name: filter-service-1
 Service State: SvcActive
 Session ID: 7
 Session uptime: 00:01:33
Service name: 1337994190863204450
 Service State: SvcActive
 Session ID: 8
 Session uptime: 00:01:33
 Accounting status: on/volume+time
 Service accounting session ID: 1:2-1322506006
 Service accounting state: Acc-Interim-Sent
 Accounting interim interval: 600
```

show network-access domain-map

Syntax **show network-access domain-map**
<statistics>

Release Information Command introduced in Junos OS Release 10.4.

Description Display domain map information.

Options **statistics**—(Optional) Display domain map statistics.

Required Privilege Level view

Related Documentation
- Verifying and Managing Domain Map Configuration on page 268

List of Sample Output show network-access domain-map statistics on page 303

Output Fields Table 40 on page 303 lists the output fields for the **show network-access domain-map statistics** command. Output fields are listed in the approximate order in which they appear.

Table 40: show network-access domain-map Output Fields

Field Name	Field Description
Matched domains	Number of usernames with domain names that are matched.
Unmatched domains	Number of usernames with domain names that are not matched.
Missing domain names	Number of usernames without a domain name.
Stripped username	Number of usernames from which the domain name has been stripped.
Default used	Number of times the default domain map is used.

Sample Output

show network-access domain-map statistics

```
user@host> show network-access domain-map statistics
General domain mapping statistics
  Matched domains: 7
  Unmatched domains: 1
  Missing domain names: 0
  Stripped username: 7
Domain statistics for domain-name: default
  Default used: 1
```

show subscribers

Syntax

show subscribers
<detail | extensive | terse>
<aci-interface-set-name *aci-interface-set-name*>
<address *address*>
<agent-circuit-identifier *agent-circuit-identifier-substring*>
<client-type *client-type*>
<count>
<interface *interface*>
<logical-system *logical-system*>
<mac-address *mac-address*>
<physical-interface *physical-interface-name*>
<profile-name *profile-name*>
<routing-instance *routing-instance*>
<stacked-vlan-id *stacked-vlan-id*>
<subscriber-state *subscriber-state*>
<user-name *user-name*>
<vci *vci-identifier*>
<vpi *vpi-identifier*>
<vlan-id *vlan-id*>

Release Information

Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description

Display information for active subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier-substring—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

client-type—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the **count** option alone or with the **address**, **client-type**, **interface**, **logical-system**, **mac-address**, **profile-name**, **routing-instance**, **stacked-vlan-id**, **subscriber-state**, or **vlan-id** options.

id—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the **show subscribers extensive** or the **show subscribers interface extensive** commands.

interface—(Optional) Display subscribers whose interface matches the specified interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is **0** through **255**.

vpi-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is **0** through **65535**.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation

- show subscribers summary on page 322
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*

List of Sample Output

show subscribers vlan-id detail on page 321
show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session) on page 321

Output Fields Table 41 on page 307 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 41: show subscribers Output Fields

Field Name	Field Description
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id* No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is **Tunnel-switched**.
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
Primary DNS Address	IP address of primary DNS server.
Secondary DNS Address	IP address of secondary DNS server.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through ND/RA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.

Table 41: show subscribers Output Fields *(continued)*

Field Name	Field Description
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface Type	Whether the subscriber interface is **Static** or **Dynamic**.
Interface Set	Internally generated name of the dynamic ACI interface set used by the subscriber session.
Interface Set Type	Interface type of the ACI interface set: **Dynamic**. This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (**Init**, **Configured**, **Active**, **Terminating**, **Tunneled**).
L2TP State	Current state of the L2TP session, **Tunneled** or **Tunnel-switched**. When the value is **Tunnel-switched**, two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
VLAN Id	VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
Agent Remote ID	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
DHCP Relay IP Address	IP address used by the DHCP relay agent.

Table 41: show subscribers Output Fields *(continued)*

Field Name	Field Description
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber service session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.

Table 41: show subscribers Output Fields *(continued)*

Field Name	Field Description
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     100                                    default:default
demux0.1073741824       100.0.0.10           WHOLESALER-CLIENT default:default
demux0.1073741825       101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001::c0:0:0:0/74    WHOLESALER-CLIENT   default:default
     *             2002::1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name
LS:RI
demux0.1073741834   0x8100.1002 0x8100.1
default:default
demux0.1073741835   0x8100.1001 0x8100.1
default:default
pp0.1073741836      61.1.1.1                   dualstackuser1@ISP1.com
```

```
default:ASP-1
*                   2041:1:1::/48
*                   2061:1:1:1::/64
pp0.1073741837      23.1.1.3                dualstackuser2@ISP1.com
default:ASP-1
*                   2001:1:2:5::/64
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1         192.168.4.1          xyz@example.com   default:default
```

show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers
Interface           IP Address/VLAN ID    User Name             LS:RI
si-2/1/0.1073741842 Tunnel-switched       ap@lts.com        default:default

si-2/1/0.1073741843 Tunnel-switched       ap@lts.com        default:default
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 100.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```

show subscribers address detail (IPv6)

```
user@host> show subscribers address 100.16.12.137 detail
```

```
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 100.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
```

```
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@jnpr.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: ap@example.com
```

```
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
```

```
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
```

```
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
...
Type: VLAN
  Logical System: default
  Routing Instance: default
  Interface: ae0.1073741824
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
```

```
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
```

```
Effective shaping-rate: 31000000k
...
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
```

```
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
```

```
Interface           IP Address/VLAN ID   User Name         LS:RI
demux0.1073741825     101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
```

```
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface           IP Address                              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail

```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

show subscribers summary

Syntax

show subscribers summary
< detail | extensive | terse>
<count>
physical-interface *physical-interface-name*
<all | logical-system *logical-system* pic | port | routing-instance *routing-instance* |slot>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display summary information for subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

count—(Optional) Display the count of total subscribers and active subscribers for any specified option.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type and LS:RI.

pic—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.

port—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

slot—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.

NOTE: **Due to display limitations, logical system and routing instance output values are truncated when necessary.**

Required Privilege Level

view

Related Documentation

- show subscribers on page 304

List of Sample Output

show subscribers summary on page 324
show subscribers summary all on page 324
show subscribers summary physical-interface on page 324
show subscribers summary physical-interface pic on page 325

show subscribers summary physical-interface port on page 325
show subscribers summary physical-interface slot on page 325
show subscribers summary pic on page 325
show subscribers summary pic (Aggregated Ethernet Interfaces) on page 326
show subscribers summary port on page 326
show subscribers summary slot on page 326
show subscribers summary terse on page 326

Output Fields Table 42 on page 323 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 42: show subscribers Output Fields

Field Name	Field Description
Subscribers by State	Number of subscribers summarized by state. The summary information includes the following: • Init—Number of subscriber currently in the initialization state. • Configured—Number of configured subscribers. • Active—Number of active subscribers. • Terminating—Number of subscribers currently terminating. • Terminated—Number of terminated subscribers. • Total—Total number of subscribers for all states.
Subscribers by Client Type	Number of subscribers summarized by client type. Client types can include DHCP, L2TP, PPP, PPPOE, STATIC-INTERFACE, and VLAN. Also displays the total number of subscribers for all client types (Total).
Subscribers by LS:RI	Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Also displays the total number of subscribers for all LS:RI combinations (Total).
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session. For aggregated Ethernet interfaces, the output of the **summary (pic | port | slot)** options prefixes the interface name with **ae0:**.
Count	Count of subscribers displayed for each PIC, port, or slot when those options are specified with the **summary** option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link.
Total Subscribers	Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id*
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.

Sample Output

show subscribers summary

```
user@host> show subscribers summary

Subscribers by State
 Init      3
 Configured    2
 Active   183
 Terminating    2
 Terminated    1

 TOTAL        191

Subscribers by Client Type
 DHCP     107
 PPP       76
 VLAN       8

 TOTAL        191
```

show subscribers summary all

```
user@host> show subscribers summary all
Subscribers by State
 Init         3
 Configured       2
 Active      183
 Terminating       2
 Terminated       1

 TOTAL          191

Subscribers by Client Type
 DHCP      107
 PPP          76
 VLAN          8

 TOTAL         191

Subscribers by LS:RI
 default:default   1
 default:ri1     28
 default:ri2     16
 ls1:default    22
 ls1:riA     38
 ls1:riB     44
 logsysX:routinstY  42

 TOTAL     191
```

show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
Subscribers by State
   Active: 3998
   Total: 3998

Subscribers by Client Type
   DHCP: 3998
```

```
   Total: 3998

Subscribers by LS:RI
   default:default: 3998
   Total: 3998
```

show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary pic

```
user@host> show subscribers summary pic
Interface           Count
ge-1/0              1000
ge-1/3              1000

Total Subscribers: 2000
```

show subscribers summary pic (Aggregated Ethernet Interfaces)

```
user@host> show subscribers summary pic
Interface           Count
ae0: ge-1/0         801
ae0: ge-1/3         801

Total Subscribers: 801
```

show subscribers summary port

```
user@host> show subscribers summary port
Interface           Count
ge-1                2000

Total Subscribers: 2000
```

show subscribers summary slot

```
user@host> show subscribers summary slot
Interface           Count
ge-1                2000

Total Subscribers: 2000
```

show subscribers summary terse

```
user@host> show subscribers summary terse
Interface           IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824   100                                   default:default
demux0.1073741824     100.0.0.10           WHOLESALER-CLIENT default:default
demux0.1073741825     101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show system subscriber-management summary

Syntax show system subscriber-management summary

Release Information Command introduced in Junos OS Release 11.1.

Description Display complete subscriber management database summary information.

Options **none**—This command has no options.

Required Privilege Level view

Related Documentation
- show database-replication statistics on page 279
- show database-replication summary on page 281

List of Sample Output show system subscriber-management summary on page 328

Output Fields Table 43 on page 327 lists the output fields for the **show system subscriber-management summary** command. Output fields are listed in the approximate order in which they appear.

Table 43: show system subscriber-management summary Output Fields

Field Name	Field Description
Graceful Restart	State of graceful Routing Engine switchover (GRES): • **Enabled** • **Disabled**
Mastership	State of the Routing Engine: • **Master** • **Standby**
Database	State of the subscriber management database: • **Available** • **Init** • **Not-available**

Table 43: show system subscriber-management summary Output Fields *(continued)*

Field Name	Field Description
Chassisd ISSU State	State of unified ISSU chassis daemon: • ABORT • DAEMON_ISSU_PREPARE • DAEMON_ISSU_PREPARE_DONE • DAEMON_SWITCHOVER_PREPARE • DAEMON_SWITCHOVER_PREPARE_DONE • FRU_ISSU • FRU_ISSU_DONE • IDLE • UNKNOWN
ISSU State	State of unified ISSU aggregate daemon: • ABORT • IDLE • PREPARE • READY • SWITCHOVER_PREPARE • SWITCHOVER_READY • UNKNOWN
ISSU Wait	Amount of time, in seconds, requested by a daemon to perform cleanup. If multiple daemons request time, the displayed value is the highest wait time requested by a daemon.

Sample Output

show system subscriber-management summary

```
user@host> show system subscriber-management summary
General:
    Graceful Restart     Enabled
    Mastership           Master
    Database             Available
    Chassisd ISSU State  DAEMON_ISSU_PREPARE
    ISSU State           PREPARE
    ISSU Wait            198
```

test aaa authd-lite user

Syntax test aaa authd-lite user *username* password *password* profile *access-profile-name*
<port *nas-port*>
<zero-stats>

Release Information Command introduced in Junos OS Release 11.2.

Description Verify authd-lite subscriber access authentication, accounting, and address allocation configuration.

Options ***username***—Specify the subscriber username to test.

password *password*—Specify the password associated with the username.

profile *access-profile-name*—Specify the access profile associated with the subscriber.

port *nas-port*—(Optional) Specify the NAS port used for the test.

zero-stats—(Optional) Specify that no accounting statistics are set for this test.

Required Privilege Level view

List of Sample Output test aaa authd-lite user on page 329

Output Fields When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show network-access aaa statistics authentication, show network-access aaa subscribers, and show subscribers commands.

The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

Sample Output

test aaa authd-lite user

The following example tests the configuration for authd-lite subscriber brady-t with a password of a11pr0 and an access profile of employee12, and displays the resulting output:

```
user@host> test aaa authd-lite user brady-t password a11pr0 profile employee12
    Authentication Grant
    ************User Attributes************
         User Name -                          brady-t
         Framed Ipv6 Prefix -                 ::/0
         Framed Ipv6 Pool -                   NULL
         Nas Ipv6 Address -                   ::
         NDRA Ipv6 Prefix -                   NULL
         Login Ipv6 Host -                    ::
         Framed Interface Id: -               0:0:0:0
         Delegated Ipv6 Prefix -              ::/0
```

```
            NDRA Ipv6 Pool -                        NULL
            User Password -                         a11pr0
            Nas Ip Address -                        0.0.0.0
            NAS Port -                              0
            Service Type-                           0
            Framed IP Address -                     0.0.0.0
            Framed IP Netmask -                     0.0.0.0
            Filter Id -                             NULL
            Framed MTU -                            0
            Reply Message -                         NULL
            Framed Route-                           not set
            Framed MTU -                            0
            Class -                                 SBR2CL          Virtual Router
Name                        NULL
            Primary DNS IP Address -                0.0.0.0
            Secondary DNS IP Address -              0.0.0.0
            Primary WINS IP Address -               0.0.0.0
            Secondary WINS IP Address -             0.0.0.0
            Ingress Statistics                      disabled
            Egress Statistics                       disabled
            Ingress Policy Name                     not set
            Engress Policy Name                     not set
            IGMP                                    disabled
            Redirect VR Name                        not set
            Service Bundle                          not set
            Framed Ip Route Tag                     not set
            LI Action                               0
            LI Interception Identifier              0
            LI Mediation Device IP Address          0.0.0.0
            LI_Mediation_Device_Port_Number         0
            Activate Service                        NULL
            Deactivate Service                      NULL
            Service Statistics                      0
            Ignore_DF_Bit -                         disabled
            IGMP Access Group Name                  not set
            IGMP Access Source Group_Name -         not set
            MLD Access Group Name                   not set
            MLD Access Source Group Name            not set
            MLD Version -                           MLD Version not set
            IGMP Version                            IGMP Version not set
            IGMP Immediate Leave -                  disabled
            MLD Immediate Leave -                   disabled
            IPv6_Ingress_Policy_Name -              not set
            IPv6_Egress_Policy_Name -               not set
            Cos_Parameter_Type -                    not set
            Service Interim Acct Interval           0
            Max Clients Per Interface               0
            Cos_Scheduler_Pmt_Type                  not set
            Session Timeout                         599999940
            NAS Port Type                           0
            Framed Pool                             NULL
            Idle Timeout                            0
        Acct-start sent
        Acct-start succeeded
        Pausing 10 seconds
        Interim-Acct sent
        Acct-interim succeeded
        Pausing 10 seconds
        Acct-stop sent
        Acct-stop succeeded
```

```
Logging out subscriber
Test complete. Exiting
```

test aaa dhcp user

Syntax

test aaa dhcp user *username*
<agent-remote-id *ari*>
<logical-system *logical-system-name*>
<mac-address *mac-address*>
<option-82 *option-82*>
<password *password*>
<profile *access-profile-name*>
<routing-instance *routing-instance-name*>
<source-address *source-address*>
<terminate-code *code-value*>

Release Information

Command introduced in Junos OS Release 11.2.
Option **terminate-code** introduced in Junos OS Release 11.4.

Description

Verify Dynamic Host Configuration Protocol (DHCP) subscriber access authentication, accounting, and address allocation configuration.

Options

username—Subscriber username to test.

agent-remote-id *ari*—(Optional) Value of the DSL Forum Agent-Remote-Id (VSA 26–2).

logical-system *logical-system-name*—(Optional) Logical system in which the subscriber is authenticated.

mac-address *mac-address*—(Optional) MAC address of the DHCP client.

option-82 *option-82*—(Optional) DHCP relay agent information option (option-82) value.

password *password*—(Optional) Password associated with the username.

profile *access-profile-name*—(Optional) Access profile associated with the subscriber.

routing-instance *routing-instance-name*—(Optional) Routing instance in which the subscriber is authenticated.

source-address *source-address*—(Optional) IP address of the outgoing interface.

terminate-code *code-value*—(Optional) Code associated with the subscriber termination.

Required Privilege Level

view

List of Sample Output

test aaa dhcp user on page 333

Output Fields

When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show network-access aaa statistics authentication, show network-access aaa subscribers, and show subscribers commands.

The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

Sample Output

test aaa dhcp user

The following example tests the configuration for DHCP subscriber esmeralda and password rch4Astar, and displays the resulting output:

```
user@host> test aaa dhcp user esmeralda password rch4Astar
    Authentication Grant
    ************Attributes***********
         User Name -                          esmeralda
         Client IP Address -                  192.168.1.2
         Client IP Netmask -                  255.255.0.0
         Reply Message                        NULL
         Primary DNS IP Address  -            0.0.0.0
         Secondary DNS IP Address  -          0.0.0.0
         Primary WINS IP Address  -           0.0.0.0
         Secondary WINS IP Address  -         0.0.0.0
         Framed Pool -                        addr_pool5
         Session Timeout -                    0
         Idle Timeout -                       0
         Service Type -                       0
         DHCP Guided Relay Server -           0
         Client Ipv6 Address -                ::
         Client Ipv6 Mask -                   null
         Framed Ipv6 Prefix -                 ::/0
         Framed Ipv6 Pool -                   not-set
         Nas Ipv6 Address -                   ::
         NDRA Ipv6 Prefix -                   not-set
         Login Ipv6 Host -                    ::
         Framed Interface Id: -               0:0:0:0
         Delegated Ipv6 Prefix -              ::/0
         Delegated Ipv6 Pool -                not-set
         User Password -                      testpw
         NAS Ip Address -                     0.0.0.0
         NAS Port -                           0
         NAS Port Type -                      5
         Dhcp Mac Address -                   AB:CD:00:00:00:01
         Dhcp GI Address -                    192.168.2.254
    Client Session Activate  request sent
    Client Session Activated
         Filter Id -                          not set
         Framed MTU -                         (null)
         Framed Route -                       not set
         IGMP -                               disabled
         Redirect VR Name -                   default
         Service Bundle -                     Null
         Ingress Policy Name -                not set
         Egress Policy Name -                 not set
         Framed Ip Route Tag -                not set
         LI Action -                          0
         LI Intercpet Id -                    0
         Med Ipaddress -                      0.0.0.0
         Med Port Number -                    0
         Ignore DF Bit -                      disabled
         IGMP Access Group Name -             not set
```

```
     IGMP Access Source Group Name -          not set
     MLD Access Group Name -                  not set
     MLD Access Source Group Name -           not set
     IGMP Version -                           IGMP Version not set
     MLD Version -                            MLD Version not set
     IGMP Immediate Leave -                   disabled
     MLD Immediate Leave -                    disabled
     IPv6 Ingress Policy Name -               not set
     IPv6 Egress Policy Name -                not set
     Cos Parameter Type -                     not set
     Cos  Scheduler Parameter Type -          not set
     Acct Session ID-                         9
     Acct Interim Interval -                  0
     Acct Type -                              0
     Ingress Statistics                       disabled
     Egress Statistics                        disabled
****Pausing 10 seconds before disconnecting the test user*********
Logging out subscriber
     Terminate Id -                           dhcp nak
Test complete. Exiting
```

test aaa ppp user

Syntax

test aaa ppp user *username*
<agent-remote-id *ari*>
<logical-system *logical-system-name*>
<password *password*>
<profile *access-profile-name*>
<routing-instance *routing-instance-name*>
<terminate-code *code-value*>

Release Information

Command introduced in Junos OS Release 11.2.
Option **terminate-code** introduced in Junos OS Release 11.4.

Description

Verify Point-to-Point Protocol (PPP) subscriber access authentication, accounting, and address allocation configuration.

Options

username—Subscriber username to test.

agent-remote-id *ari*—(Optional) Value of the DSL Forum Agent-Remote-Id (VSA 26–2).

logical-system *logical-system-name*—(Optional) Logical system in which the subscriber is authenticated.

password *password*—(Optional) Password associated with the username.

profile *access-profile-name*—(Optional) Access profile associated with the subscriber.

routing-instance *routing-instance-name*—(Optional) Routing instance in which the subscriber is authenticated.

terminate-code *code-value*—(Optional) Code associated with the subscriber termination.

Required Privilege Level

view

List of Sample Output

test aaa ppp user on page 336
test aaa ppp user (tunneled user) on page 337

Output Fields

When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show network-access aaa statistics authentication, show network-access aaa subscribers, and show subscribers commands.

The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

Sample Output

test aaa ppp user

The following example tests the configuration for PPP subscriber jilldoe and password 92&tDcb, and displays the resulting output:

```
user@host> test aaa ppp user jilldoe password 92&tDcb
    Authentication Grant
    ************User Attributes************
         User Name -                          jilldoe
         Client IP Address -                  192.168.1.5
         Client IP Netmask -                  255.255.0.0
         Virtual Router Name -                default
         Reply Message -                      NULL
         Primary DNS IP Address -             0.0.0.0
         Secondary DNS IP Address -           0.0.0.0
         Primary WINS IP Address -            0.0.0.0
         Secondary WINS IP Address -          0.0.0.0
         Framed Pool -                        addr_pool3
         Session Timeout -                    0
         Idle Timeout -                       0
         Service Type -                       0
         Client Ipv6 Address -                ::
         Client Ipv6 Mask -                   null
         Framed Ipv6 Prefix -                 ::/0
         Framed Ipv6 Pool -                   not-set
         Nas Ipv6 Address -                   ::
         NDRA Ipv6 Prefix -                   not-set
         Login Ipv6 Host -                    ::
         Framed Interface Id: -               0:0:0:0
         Delegated Ipv6 Prefix -              ::/0
         Delegated Ipv6 Pool -                not-set
         User Password -                      92&tDcb
         CHAP Password -                      NULL
         NAS Ip Address -                     0.0.0.0
         NAS Port -                           0
         NAS Port Type -                      5
    Client Session Activate request sent
    Client Session Activated
         Filter Id -                          not set
         Framed MTU -                         (null)
         Framed Route -                       not set
         Ingress Policy Name -                not set
         Egress Policy Name -                 not set
         IGMP -                               disabled
         Redirect VR Name -                   default
         Service Bundle -                     Null
         Framed Ip Route Tag -                not set
         LI Action -                          0
         LI Intercpet Id -                    0
         Med Ipaddress -                      0.0.0.0
         Med Port Number -                    0
         Ignore DF Bit -                      disabled
         IGMP Access Group Name -             not set
         IGMP Access Source Group Name -      not set
         MLD Access Group Name -              not set
         MLD Access Source Group Name -       not set
         IGMP Version -                       IGMP Version not set
         MLD Version -                        MLD Version not set
```

```
        IGMP Immediate Leave -                  disabled
        MLD Immediate Leave -                   disabled
        IPv6 Ingress Policy Name -              not set
        IPv6 Egress Policy Name -               not set
        Cos Parameter Type -                    not-set
        Cos  Scheduler Parameter Type -         not-set
        Acct Session ID-                        8
        Acct Interim Interval -                 0
        Acct Type -                             0
        Ingress Statistics                      disabled
        Egress Statistics                       disabled
    ****Pausing 10 seconds before disconnecting the test user*********
    Logging out subscriber
        Terminate Id -                          ppp lcp-no-peer-mru
    Test complete. Exiting
```

test aaa ppp user (tunneled user)

The following example tests the configuration for PPP tunneled subscriber accounting14, with password bncntr14 and access profile finance-b, and displays the resulting output:

```
user@host> test aaa ppp user accounting14 password bncntr14 profile finance-b
    Authentication Grant with Tunnel Attributes
    ************Tunnel Attributes***********
        ****Tunnel Definiton -                  1
            Tunnel Medium           -           1
            Tunnel Type             -           3
            Tunnel Max Sessions     -           100
            Tunnel Server Endpoint  -           1.2.3.4
            Tunnel Client Endpoint  -           2.3.4.5
            Tunnel Server AuthId    -           rt1
            Tunnel Client AuthId    -           ts1
            Tunnel Password         -           radius
            Tunnel Assignment Id    -           til
            Tunnel Logical System   -
            Tunnel Routing Instance -
    ****Pausing 10 seconds before disconnecting the test user*********
    Logging out subscriber
        Terminate Id -                          l2tp
session-receive-cdn-avp-bad-hidden
    Test complete. Exiting
```

PART 4

Troubleshooting

CHAPTER 12

Acquiring Troubleshooting Information

Tracing Subscriber Management Database Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **smid**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

   You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of subscriber management database tracing operations:

1. Configure a trace log filename.

   See "Configuring the Subscriber Management Database Trace Log Filename" on page 342.
2. Configure the number and size of trace logs.

   See "Configuring the Number and Size of Subscriber Management Database Log Files" on page 343.
3. Configure user access to trace logs.

   See "Configuring Access to the Subscriber Management Database Log File" on page 343.
4. Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged" on page 344.
5. Configure flags to specify which events are logged.

   See "Configuring the Subscriber Management Database Tracing Flags" on page 344.

Configuring the Subscriber Management Database Trace Log Filename

By default, the name of the file that records trace output for the subscriber management database is **smid**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.


```
[edit system services subscriber-management traceoptions]
user@host# set file smi_logfile_1
```

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

Configuring the Number and Size of Subscriber Management Database Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_1 _logfile_1 files 20 size 2097152
```

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

Configuring Access to the Subscriber Management Database Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_1 _logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

  ```
  [edit system services subscriber-management traceoptions]
  user@host# set file smi_1 _logfile_1 no-world-readable
  ```

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

  ```
  [edit system services subscriber-management traceoptions]
  user@host# set file smi_1 _logfile_1 match regex
  ```

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

Configuring the Subscriber Management Database Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

  ```
  [edit system services subscriber-management traceoptions]
  user@host# set flag flag
  ```

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

Tracing Subscriber Management Session Database Replication Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database replication operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **bdbrepd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

   You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of subscriber management database replication tracing operations:

1. Configure a trace log filename.

   See "Configuring the Subscriber Management Session Database Replication Trace Log Filename" on page 345.
2. Configure the number and size of trace logs.

   See "Configuring the Number and Size of Subscriber Management Session Database Replication Log Files" on page 346.
3. Configure user access to trace logs.

   See "Configuring Access to the Subscriber Management Session Database Replication Log File" on page 346.
4. Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged" on page 347.
5. Configure flags to specify which events are logged.

   See "Configuring the Subscriber Management Session Database Replication Tracing Flags" on page 347.

Configuring the Subscriber Management Session Database Replication Trace Log Filename

By default, the name of the file that records trace output for the subscriber management database is **bdbrepd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

  ```
  [edit system services database-replication traceoptions]
  user@host# set file bdbrep_logfile_1
  ```

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

Configuring the Number and Size of Subscriber Management Session Database Replication Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

  ```
  [edit system services database-replication traceoptions]
  user@host# set file bdrep_1 _logfile_1 files 20 size 2097152
  ```

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

Configuring Access to the Subscriber Management Session Database Replication Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

  ```
  [edit system services database-replication traceoptions]
  user@host# set file bdrep_1 _logfile_1 world-readable
  ```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

  ```
  [edit system services database-replication traceoptions]
  user@host# set file bdrep_1 _logfile_1 no-world-readable
  ```

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

  ```
  [edit system services database-replication traceoptions]
  user@host# set file bdrep_1 _logfile_1 match regex
  ```

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

Configuring the Subscriber Management Session Database Replication Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

  ```
  [edit system services database-replication traceoptions]
  user@host# set flag flag
  ```

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

   ```
   [edit]
   set system syslog archive size 100m files 25
   set system auto-configuration traceoptions file filename
   set system auto-configuration traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions level all
   set protocols ppp-service traceoptions flag all
   set protocols ppp traceoptions file filename size 100m files 25
   set protocols ppp traceoptions level all
   set protocols ppp traceoptions flag all
   set protocols ppp monitor-session all
   set interfaces pp0 traceoptions flag all
   set demux traceoptions file filename size 100m files 25
   set demux traceoptions level all
   set demux traceoptions flag all
   set system processes dhcp-service traceoptions file filename
   set system processes dhcp-service traceoptions file size 100m
   set system processes dhcp-service traceoptions file files 25
   set system processes dhcp-service traceoptions flag all
   set class-of-service traceoptions file filename
   set class-of-service traceoptions file size 100m
   set class-of-service traceoptions flag all
   set class-of-service traceoptions file files 25
   set routing-options traceoptions file filename
   set routing-options traceoptions file size 100m
   set routing-options traceoptions flag all
   set routing-options traceoptions file files 25
   set interfaces traceoptions file filename
   set interfaces traceoptions file size 100m
   set interfaces traceoptions flag all
   set interfaces traceoptions file files 25
   set system processes general-authentication-service traceoptions file filename
   set system processes general-authentication-service traceoptions file size 100m
   set system processes general-authentication-service traceoptions flag all
   set system processes general-authentication-service traceoptions file files 25
   ```

2. Copy the relevant statements into a text file and modify the log filenames as you want.

3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

Related Documentation

- Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support on page 349

Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support

Problem You have collected logs on your device and need to send them to Juniper Technical Support. This topic shows you how to compress the logs into a single file for each Routing Engine to more conveniently send the logs.

Solution You can compress all the log files in the **/var/log** directories of the master and backup (if present) Routing Engines into a single **tgz** file for each Routing Engine, which enables you to send the logs to JTAC in a convenient package. You can use either the CLI or the command shell to perform these tasks; because of its ease of use, only the CLI version is shown here.

1. Access the device through the management IP address or console, typically on the master Routing Engine, RE0.

   ```
   user@host>
   ```

2. Archive and compress all the log files on RE0 and put them in **/var/tmp**.

   ```
   user@host> file archive compress source /var/log/* destination /var/tmp/re0.tgz
   /usr/bin/tar: Removing leading `/' from member names
   ```

3. Confirm that the compressed archive file has been created.

   ```
   user@host> file list /var/tmp
   baseline-config.conf
   gres-tp
   idp_license_info
   install
   jinstall-12.2-20120328.0-domestic-signed.tgz
   krt_gencfg_filter.txt
   preinstall_boot_loader.conf
   re0.tgz
   rtsdb
   ```

```
sec-download
vi.recover
```

On devices with a single Routing Engine, skip to Step 10.

4. Log in to the backup Routing Engine, RE1, and access the CLI.

NOTE: *1* is appended to the hostname in the prompt to signify that you are on RE1.

```
user@host> request routing-engine login backup
% cli
user@host11>
```

5. Archive and compress all the log files on RE1 and put them in **/var/tmp**.

```
user@host1> file archive compress source /var/log/* destination /var/tmp/re1.tgz
/usr/bin/tar: Removing leading `/' from member names
```

6. Confirm that the compressed archive file has been created.

```
user@host1> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re1.tgz
rtsdb
sec-download
vi.recover
%
```

7. Exit the remote login to the backup Routing Engine to return to the master Routing Engine. Note that the previously appended *1* is removed from the hostname in the prompt to signify that you are back on RE0.

```
user@host1> exit
rlogin: connection closed

user@host1>
```

8. Copy the compressed archive file from RE1 to RE0.

```
user@host> file copy re1:/var/tmp/re1.tgz /var/tmp
```

9. Confirm the presence of the copied file.

```
user@host> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re0.tgz
re1.tgz
rtsdb
```

```
sec-download
vi.recover
%
```

10. Copy the files directly from the master Routing Engine to any local host using FTP, SCP, JWEB, or (on some devices) a mounted USB.

Related Documentation

- Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 348

CHAPTER 13

Troubleshooting Configuration Statements

traceoptions (Subscriber Management)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit system services subscriber-management]

Release Information Statement introduced in Junos OS Release 11.1.

Description Define tracing operations for subscriber management interface processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **database**—Trace database events.
- **general**—Trace general events.
- **issu**—Trace unified ISSU events.
- **server**—Trace server events.
- **session-db**—Trace session database interactions.
- **ui**—Trace user interface events.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 341

traceoptions (Subscriber Session Database Replication)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit system services database-replication]

Release Information Statement introduced in Junos OS Release 9.3.

Description Define tracing operations for subscriber management session database replication processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **database**—Trace database events.
- **general**—Trace general flow.
- **mirror**—Trace mirroring events.
- **replication**—Trace database replication events.
- **server**—Trace server events.
- **session-db**—Trace session database interactions.
- **ui**—Trace user interface events.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to

indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 344

PART 5

Index

Index

Symbols

A

B

C

D

N

O

P

R

S

T

U

V

W