JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

Remote Access Services

Release
14.1.x

Published: 2012-12-20

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

JunosE™ Software for E Series™ Broadband Services Routers Remote Access Services
Release 14.1.x

Revision History
December 2012—FRS JunosE 14.1.x

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

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

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

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

Audience

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

E Series and JunosE Text and Syntax Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

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

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

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

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

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

Obtaining Documentation

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

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

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

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

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

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

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Understanding Remote Access

Remote Access Overview

Broadband Remote Access Server (B-RAS) is an application running on your router that:

- Aggregates the output from digital subscriber line access multiplexers (DSLAMs)
- Provides user Point-to-Point Protocol (PPP) sessions or IP-over-Asynchronous Transfer Mode (ATM) sessions
- Enforces quality of service (QoS) policies
- Routes traffic into an Internet service provider's (ISP's) backbone network

A DSLAM collects data traffic from multiple subscribers into a centralized point so that it can be uploaded to the router over an ATM connection via a DS3, OC3, E3, or OC12 link.

The router provides the logical termination for PPP sessions, as well as the interface to authentication and accounting systems.

The following sections provide an overview of remote access:

B-RAS Data Flow

The router performs several tasks for a digital subscriber line (DSL) PPP user to establish a PPP connection. This is an example of the way B-RAS data might flow:

1. Authenticate the subscriber using RADIUS authentication.
2. Assign an IP address to the PPP/IP session via RADIUS, local address pools, or Dynamic Host Configuration Protocol (DHCP).

3. Terminate the PPP encapsulation or tunnel a PPP session.
4. Provide user accounting via RADIUS.

NOTE: For information about configuring RADIUS attributes see the *Configuring RADIUS Attributes* chapter..

Configuring IP Addresses for Remote Clients

A remote client can obtain an IP address from one of the following:

- RADIUS server
- Local address server
- DHCP proxy client and server
- DHCP relay agent (Bridged IP only)
- DHCP local server
- DHCP external server

For information about configuring DHCP support on the E Series router, see the *DHCP Overview* chapter.

For information about how to configure a RADIUS server, see your RADIUS server documentation.

AAA Overview

Collectively, authentication, authorization, and accounting are referred to as AAA. Each has an important but separate function.

- Authentication—Determines who the user is, then determines whether that user should be granted access to the network. The primary purpose is to prevent intruders from networks. It uses a database of users and passwords.
- Authorization—Determines what the user is allowed to do by giving network managers the ability to limit network services to different users.
- Accounting—Tracks what the user did and when they did it. You can use accounting for an audit trail or for billing for connection time or resources used.

Central management of AAA means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

Related Documentation

- Remote Access Configuration Tasks on page 89

Remote Access Platform Considerations

B-RAS services are supported on all E Series routers.

For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the Juniper Networks E120 and E320 Broadband Services Routers.
- B-RAS Protocol Support on page 5

B-RAS Protocol Support

The E Series router supports the following protocols for B-RAS services:

- PPP
- PPP over Ethernet (PPPoE)
- Bridged Ethernet
- Layer 2 Tunneling Protocol (L2TP), both L2TP access concentrator (LAC) and L2TP network server (LNS)

Remote Access References

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

- RFC 2748—The COPS (Common Open Policy Service) Protocol (January 2000)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)
- RFC 3084—COPS Usage for Policy Provisioning (COPS-PR) (March 2001)
- RFC 3159—Structure of Policy Provisioning Information (SPPI) (August 2001)
- RFC 3198—Terminology for Policy-Based Management (November 2001)
- RFC 3317—Differentiated Services Quality of Service Policy Information Base (DIFFSERV-PIB)
- RFC 3318—Framework Policy Information Base (March 2003)

JunosE Release Notes, *Appendix A*, *System Maximums*—Refer to the Release Notes corresponding to your software release for information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers.

DHCP Features

DHCP provides a mechanism through which computers using Transmission Control Protocol/IP (TCP/IP) can obtain an IP address and protocol configuration parameters automatically from a DHCP server on the network.

The E Series router provides support for the following DHCP features:

- DHCP proxy client
- DHCP relay agent
- DHCP relay proxy
- DHCP local server
- DHCP external server

Related Documentation

- DHCP Overview Information

CHAPTER 2

How the Domain Map Feature Works

Domain Name Aliases Overview

You can translate an original domain name to a new domain name via the **translate** command. The command allows you to create domain name aliases; that is, the grouping of multiple domain names into a single domain name. You can partition PPP subscribers with the same domain into separate domains, based on the PPP interface.

NOTE: **Partitioning subscribers does not cause modification of a user's name or domain.**

When you use aliases, you greatly simplify the configuration process. When there are a large number of domains and you use aliases, it reduces the configuration volume, thus requiring less NVS and memory usage.

Overview of Mapping a User Domain to a Virtual Router

You can configure RADIUS authentication, accounting, and local address pools for a specific virtual router and then map a user domain to that virtual router.

The router keeps track of the mapping between domain names and virtual-routers. Use the **aaa domain-map** command to map a user domain to a virtual router.

NOTE: **This domain name is not the NT domain sometimes found on the Dialup Networking dialog box.**

When the router is configured to require authentication of a PPP user, the router checks for the appropriate user domain-name-to-virtual-router mapping. If it finds a match, the router sends a RADIUS authentication request to the RADIUS server configured for the specific virtual router.

The following sections describe how to map a user domain to a virtual router:

Mapping User Requests Without a Valid Domain Name

You can create a mapping between a domain name called **default** and a specific virtual router so that the router can map user names that contain a domain name that does not have an explicit map.

If a user request is submitted with a domain name for which the router cannot find a match, the router looks for a mapping between the domain name **default** and a virtual router. If a match is found, the user's request is processed according to the RADIUS server configured for the named virtual router. If no entry is found that maps **default** to a specific virtual router, the router sends the request to the RADIUS server configured on the default virtual router.

Mapping User Requests Without a Configured Domain Name

You can map a domain name called **none** to a specific virtual router so that the router can map user names that do not contain a domain name.

If a user request is submitted without a domain name, the router looks for a mapping between the domain name **none** and a virtual router. If a match is found, the user's request is processed according to the RADIUS server configured for the named virtual router. If the router does not find the domain name **none**, it checks for the domain name **default**. If no matching entries are found, the router sends the request to the server configured on the default virtual router.

Using DNIS

The E Series router supports dialed number identification service (DNIS). With DNIS, if users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing.

NOTE: For DNIS to work, the router must be acting as the LNS. Also, the phone number configured in the **aaa domain-map** command must be an exact match to the value passed by L2TP in the called number AVP (AVP 21).

For example, as specified in the following sequence, a user calling 9785551212 would be terminated in vrouter_88, while a user calling 8005554433 is terminated in vrouter_100.

```
host1(config)#aaa domain-map 9785551212 vrouter_88
host1(config)#aaa domain-map 8005554433 vrouter_100
```

Redirected Authentication

Redirected authentication provides a way to offload AAA activity on the router, by providing the domain-mapping-like feature remotely on the RADIUS server. Redirected authentication works as follows:

1. The router sends an authentication request (in the form of a RADIUS access-request message) to the RADIUS server that is configured in the default VR.
2. The RADIUS server determines the user's AAA VR context and returns this information in a RADIUS response message to the router.
3. The router then behaves in similar fashion as if it had received the VR context from the local domain map.

To maintain local control, the only VR allowed to redirect authentication is the default VR. Also, to prevent loopbacks, the redirection may occur only once to a non-default VR.

To maintain flexibility, the redirection response may include idle time or session attributes that are considered as default unless the redirected authentication server overrides them. For example, if the RADIUS server returns the VR context along with an idle timeout attribute with the value set to 20 minutes, the router uses this idle timeout value unless the RADIUS server configured in the VR context returns a different value.

Since the router supports the RADIUS User-Name attribute [1] in the RADIUS response message, the default VR RADIUS server may override the user's name (this can be a stripped name or an entirely different name). Overriding is useful for the case when the user enters a login name containing a domain name that is significant only to the RADIUS server in the default VR.

IP Hinting

You can allocate an address before authentication of PPP sessions. This address is included in the Access-Request sent to the authentication server as an IP address hint.

Related Documentation

- Domain Name and Realm Name Overview on page 9

Domain Name and Realm Name Overview

To provide flexibility in how the router handles different types of usernames, the software lets you specify the part of a username to use as the domain name, how the domain name is designated, and how the router parses names. It also allows you to set whether or not the router strips the domain name from the username before it sends the username to the RADIUS server.

By default, the router parses usernames as follows:

realmName/personalName@domainName

The string to the left of the forward slash (/) is the realm name, and the string to the right of the at-symbol (@) is the domain name. For example, in the username juniper/jill@abc.com, juniper is the realm name and abc.com is the domain name.

The router allows you to:

- Use the realm name as the domain name.
- Use delimiters other than / to designate the realm name.
- Use delimiters other than @ to designate the domain name.
- Use either the domain or the realm as the domain name when the username contains both a realm and domain name.
- Change the direction in which the router searches for the domain name or the realm name.

To provide these features, the router allows you to specify delimiters for the domain name and realm name. You can use up to eight one-character delimiters each for domain and realm names. The router also lets you specify how it parses usernames to determine which part of a username to use as the domain name.

The following sections describe domain name and realm name:

Using the Realm Name as the Domain Name

Typically, a realm appears before the user field and is separated with the / character; for example, usEast/jill@abc.com. To use the realm name usEast rather than abc.com as the domain name, set the realm name delimiter to /. For example:

```
host1(config)#aaa delimiter realmName /
```

This command causes the router to use the string to the left of the / as the domain name. If the realm name delimiter is null (the default), the router will not search for the realm name.

Using Delimiters Other Than @

You can set up the router to recognize delimiters other than @ to designate the domain name. Suppose there are two users: bob@abc.com and pete!xyz.com, and you want to use both of their domain names. In this case you would set the domain name delimiter to @ and !. For example:

```
host1(config)#aaa delimiter domainName @!
```

Using Either the Domain or the Realm as the Domain Name

If the username contains both a realm name and a domain name delimiter, you can use either the domain name or the realm name as the domain name. As previously mentioned, the router treats usernames with multiple delimiters as though the realm name is to the left of the realm delimiter and the domain name is to the right of the domain delimiter.

If you set the parse order to:

- domain-first—The router searches for a domain name first. For example, for username usEast/lori@abc.com, the domain name is abc.com.
- realm-first—The router searches for a realm name first and uses the realm name as the user's domain name. For username usEast/lori@abc.com, the domain is usEast.

For example, if you set the delimiter for the realm name to / and set the delimiter for the domain name to @, the router parses the realm first by default. The username usEast/lori@abc.com results in a domain name of usEast. To cause the parsing to return abc.com as the domain, enter the **aaa parse-order domain-first** command.

Specifying the Domain Name or Realm Name Parse Direction

You can specify the direction—either left to right or right to left—in which the router performs the parsing operation when identifying the realm name or domain name. This feature is particularly useful if the username contains nested realm or domain names. For example, for a username of userjohn@abc.com@xyz.com, you can identify the domain as either abc.com@xyz.com or as xyz.com, depending on the parse direction that you specify.

You use either the **left-to-right** or **right-to-left** keywords with one of the following keywords to specify the type of search and parsing that the router performs:

- **domainName**—The router searches for the next domain delimiter value in the direction specified. When it reaches a delimiter, the router uses anything to the right of the delimiter as the domain name. Domain parsing is from right to left by default.
- **realmName**—The router searches for the next realm delimiter value in the direction specified. When it reaches a delimiter, the router uses anything to the left of the delimiter as the realm name. Realm parsing is from left to right by default.
- Example

  host1(config)#aaa parse-direction domainName left-to-right

Stripping the Domain Name

The router provides feature that strips the domain name from the username before it sends the name to the RADIUS server in an Access-Request message. You can enable or disable this feature using the **strip-domain** command.

By default, the domain name is the text after the last @ character. However, if you changed the domain name parsing using the **aaa delimiter**, **aaa parse-order**, or **aaa parse direction** commands, the router strips the domain name and delimiter that result from the parsing.

Stripping the Domain Name Per Virtual Router

The **aaa domain-map** command maps a domain name to a virtual router. It determines the authentication and accounting access for all subscribers belonging to a particular domain. However, if a subscriber profile is configured for a virtual router using the **ppp authentication** command, the authentication for the virtual router configured at the profile level takes priority over the one configured at the domain level. If multiple profiles from the same domain are being used, the subscribers may end up in different virtual routers for authentication.

In such a scenario, you can use the **aaa strip-domain** command to strip a part of the user name of the subscriber. The resulting user name is then used as the new user name for that subscriber for RADIUS authentication and accounting.

NOTE: **The aaa strip-domain command can be configured on non-default virtual routers only.**

Subscriber User Name for RID, CoA Requests, and Lawful Intercepts When Strip Domain Is Enabled

When strip domain is enabled for a virtual router, the user name used to identify the subscriber session for RADIUS Initiated Disconnect (RID), Change of Authorization (CoA), and lawful intercepts requests is the same as the subscriber user name sent to RADIUS server for authentication.

For example, if a subscriber with user name user1@123.com$test1 has a resulting user name of user1@123.com due to the strip domain configuration, then the user name for all the incoming RID and CoA requests and the lawful intercept requests is user1@123.com.

This new user name, which has been used for RADIUS server authentication, is used for displaying subscriber information using **show subscribers** and **logout subscribers** commands.

Using the Strip Domain Functionality Per Virtual Router When Strip Domain Is Enabled for an AAA Domain Map

When strip domain is enabled for an AAA domain map using the **strip-domain enable** command in the Domain Map Configuration mode, the strip domain configured for a virtual router may cause the user name stripping to happen twice depending on the configuration.

For example, consider a subscriber with user name user1@test.com$test1$test2. Consider the following configurations for a domain map:

```
host1(config)#aaa domain-map test2
host1(config-domain-map)#strip-domain enable
```

The following has also been configured on the non-default virtual router:

```
host1(config)#aaa strip-domain enable
host1(config)#aaa strip-domain delimiter domainname $
```

In this example, when the domain name is stripped for the subscriber with user name user1@test.com$test1$test2, the resulting string that is sent for RADIUS authentication is user1. Thus, when strip domain is configured for a domain map as well as a non-default virtual router, depending on the configurations, the domain name may get stripped twice, once at the virtual router level and then at the domain map level.

In order to prevent the domain name from being stripped twice for the same subscriber, you must ensure that the strip domain functionality is configured appropriately for the domain map and for the non-default virtual router.

Redirected Authentication When Strip Domain Is Enabled

Strip domain configured on a virtual router does not work in case of a redirected authentication. In an authentication redirection, the RADIUS server sends an access-accept message for a subscriber from the virtual router on which the subscriber is already authenticated.

For example, on a virtual router vr1, we have configured the aaa strip-domain. A subscriber with user name user1@123.com is already authenticated on vr1 using the RADIUS server authentication. Now, if you send an access request message trying to authenticate the same subscriber on vr1, the access request message carries the original user name, user1@123.com, and renders strip domain ineffective during authentication redirection.

Related Documentation

- Example: Domain Name and Realm Name on page 195
- Example: Stripping Domain Name Per Virtual Router for RADIUS Server Authentication on page 196

CHAPTER 3

Understanding Authentication and Accounting Servers Functions

RADIUS Authentication and Accounting Servers Configuration Overview

The number of RADIUS servers you can configure depends on available memory.

The order in which you configure servers determines the order in which the router contacts those servers on behalf of clients.

Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The RADIUS server uses the configured IP address, the UDP port number, and the secret key to make the connection. The RADIUS client waits for a response for a configurable timeout period and then retransmits the request. The RADIUS client retransmits the request for a user-configurable retry limit.

- If there is no response from the primary RADIUS server, the RADIUS client submits the request to the secondary RADIUS server using the timeout period and retry limit configured for the secondary RADIUS server.
- If the connection attempt fails for the secondary RADIUS server, the router submits the request to the tertiary server and so on until it either is granted access on behalf of the client or there are no more configured servers.
- If another authentication server is not configured, the router attempts the next method in the method list; for accounting server requests, the information is dropped.

For example, suppose that you have configured the following authentication servers: Auth1, Auth2, Auth3, Auth4, and Auth5. Your router attempts to send an authentication request to Auth1. If Auth1 is unavailable, the router submits the request to Auth2, then Auth3, and so on until an available server is found. If Auth5, the last configured authentication server, is not available, the router attempts the next method in the methods list. If the only method configured is RADIUS, then the router notifies the client that the request has been denied.

The following sections explain how to configure RADIUS authentication and accounting servers:

Server Access

The router offers two options by which servers are accessed:

- Direct—The first authentication or accounting server that you configure is treated as the primary authentication or accounting server, the next server configured is the secondary, and so on.
- Round-robin—The first configured server is treated as a primary for the first request, the second server configured as primary for the second request, and so on. When the router reaches the end of the list of servers, it starts again at the top of the list until it comes full cycle through the list.

Use the **radius algorithm** command to specify the server access method.

When you configure the first RADIUS accounting server, a RADIUS Acct-On message is sent. When you delete the last accounting server, a RADIUS Acct-Off message is sent.

Server Request Processing Limit

You can configure RADIUS authentication servers and accounting servers to use different UDP ports on the router. This enables the same IP address to be used for both an authentication server and an accounting server. However, you cannot use the same IP address for multiple authentication servers or for multiple accounting servers.rs.

NOTE: For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JunosE Release Notes*, *Appendix A*, *System Maximums*.

The E Series router listens to a range of UDP source (or local) ports for RADIUS responses. Each UDP source port supports a maximum of 255 RADIUS requests. When the 255 per-port limit is reached, the router opens the next source port. When the **max-sessions** command limit is reached, the router submits the request to the next configured server.

Table 3 on page 17 lists the range of UDP ports the router uses for each type of RADIUS request.

Table 3: Local UDP Port Ranges by RADIUS Request Type

RADIUS Request Type	ERX310, ERX710, ERX1410, and E120 Broadband Services Routers	ERX1440 and E320 Broadband Services Routers
RADIUS authentication	50000–50124	50000–50124
RADIUS accounting	50125–50249	50125–50499
RADIUS preauthentication	50250–50374	50500–50624
RADIUS route-download	50375–50500	50625–50749

Authentication and Accounting Methods

When you configure AAA authentication and accounting services for your B-RAS environment, one important task is to specify the authentication and accounting method used. The JunosE Software gives you the flexibility to configure authentication or accounting methods based on the type of subscriber. This feature allows you to enable RADIUS authentication for some subscribers, while disabling authentication completely for other subscribers. Similarly, you can enable RADIUS accounting for some subscribers, but no accounting for others. For example, you might use RADIUS authentication for ATM 1483 subscribers, while granting IP subscriber management interfaces access without authentication (using the **none** keyword).

You can specify the authentication or accounting method you want to use, or you can specify multiple methods in the order in which you want them used. For example, if you specify the **radius** keyword followed by the **none** keyword when configuring authentication, AAA initially attempts to use RADIUS authentication. If no RADIUS servers are available, AAA uses no authentication. The JunosE Software currently supports **radius** and **none** as accounting methods and **radius**, **none**, and **local** as authentication methods. See "Local Authentication Servers Configuration Overview" on page 19 for information about local authentication.

You can configure authentication and accounting methods based on the following types of subscribers:

- ATM 1483
- Tunnels (for example, L2TP tunnels)
- PPP
- RADIUS relay server
- IP subscriber management interfaces

NOTE: IP subscriber management interfaces are static or dynamic interfaces that are created or managed by the JunosE Software's subscriber management feature.

Supporting Exchange of Extensible Authentication Protocol Messages

Extensible Authentication Protocol (EAP) is a protocol that supports multiple methods for authenticating a peer before allowing network layer protocols to transmit over the link. JunosE Software supports the exchange of EAP messages between JunosE applications, such as PPP, and an external RADIUS authentication server.

The JunosE Software's AAA service accepts and passes EAP messages between the JunosE application and the router's internal RADIUS authentication server. The internal RADIUS authentication server, which is a RADIUS client, provides EAP pass-through—the RADIUS client accepts the EAP messages from AAA, and sends the messages to the external RADIUS server for authentication. The RADIUS client then passes the response from the external RADIUS authentication server back to the AAA service, which then sends a response to the JunosE application. The AAA service and the internal RADIUS authentication service do not process EAP information—both simply act as pass-through devices for the EAP message.

The router's local authentication server and TACACS+ authentication servers do not support the exchange of EAP messages. These type of servers deny access if they receive an authentication request from AAA that includes an EAP message. EAP messages do not affect the **none** authentication configuration, which always grants access.

The local RADIUS authentication server uses the following RADIUS attributes when exchanging EAP messages with the external RADIUS authentication server:

- Framed-MTU (attribute 12)—Used if AAA passes an MTU value to the internal RADIUS client
- State (attribute 24)—Used in Challenge-Response messages from the external server and returned to the external server on the subsequent Access-Request
- Session-Timeout (attribute 27)—Used in Challenge-Response messages from the external server
- EAP-Message (attribute 79)—Used to fragment EAP strings into 253-byte fragments (the RADIUS limit)
- Message-Authenticator (attribute 80)—Used to authenticate messages that include an EAP-Message attribute

For additional information on configuring PPP to use EAP authentication, see *JunosE Link Layer Configuration Guide* .

Immediate Accounting Updates

You can use the **aaa accounting immediate-update** command to configure immediate accounting updates on a per-VR basis. If you enable this feature, the E Series router sends an Acct-Update message to the accounting server immediately on receipt of a response (ACK or timeout) to the Acct-Start message.

This feature is disabled by default. Use the **enable** keyword to enable immediate updates and the **disable** keyword to halt them.

The accounting update contains 0 (zero) values for the input/output octets/packets and 0 (zero) for uptime. If you have enabled duplicate or broadcast accounting, the accounting update goes to both the primary virtual router context and the duplicate or broadcast virtual router context.

Duplicate and Broadcast Accounting

Normally, the JunosE Software sends subscriber-related AAA accounting information to the virtual router that authenticates the subscriber. If an operational virtual router is configured that is different from the authentication router, it also receives the accounting information. You can optionally configure duplicate or broadcast AAA accounting, which sends the accounting information to additional virtual routers simultaneously. The accounting information is always sent to the authenticating virtual router. The accounting information is sent to the operational virtual router only if duplicate accounting is not enabled and if authenticating virtual router is different than the operational virtual router.

Both the duplicate and broadcast accounting features are supported on a per-virtual router context, and enable you to specify particular accounting servers that you want to receive the accounting information.

For example, you might use broadcast accounting to send accounting information to a group of your private accounting servers. Or you might use duplicate accounting to send the accounting information to a customer's accounting server.

- Duplicate accounting—Sends the accounting information to a particular virtual router
- Broadcast accounting—Sends the accounting information to a group of virtual routers. An accounting virtual router group can contain up to four virtual routers and the E Series router supports a maximum of 100 virtual router groups. The accounting information continues to be sent to the duplicate accounting virtual router, if one is configured.

UDP Checksums

Each virtual router on which you configure B-RAS is enabled to perform UDP checksums by default. You can disable and reenable UDP checksums.

Related Documentation

- Remote Access Configuration Tasks on page 89

Local Authentication Servers Configuration Overview

The AAA local authentication server enables the E Series router to provide local PAP and CHAP user authentication for subscribers. The router also provides limited authorization, using the IP address, IP address pool, and operational virtual router parameters. When a subscriber logs on to the E Series router that is using local authentication, the subscriber is authenticated against user entries in a local user database; the optional parameters are assigned to subscribers after the subscriber is authenticated.

Related Documentation

- Creating the AAA Local Authentication Environment on page 99
- Creating AAA Local User Databases on page 100

Tunnel Subscriber Authentication Configuration Overview

When a AAA domain map includes any tunnel configuration, users in this domain are considered to be tunnel subscribers. By default, any such subscriber is granted access without being authenticated by the authentication server. Access is granted even when the user provides an invalid username and password. The tunnel configuration for the subscriber comes from the AAA domain map.

For example, if the authentication protocol for a AAA domain map is RADIUS, AAA grants access to subscribers from this domain immediately without sending access requests to the configured RADIUS server. Because of this behavior, these subscribers cannot get any additional control attributes from the authentication server. This reduces your ability to manage the tunnel subscribers.

In this default situation, if you want the domain subscribers to be managed by the authentication server for any control attribute, then that domain map cannot have any tunnel configuration. Typically, this means you must configure the subscriber individually.

You can use the **tunnel-subscriber authentication** command to get around this limitation. When you enable authentication with this command, access requests for the tunnel subscribers in the domain are sent to the configured authentication server. When the access replies from authentication server are processed, various user attributes from the server can be applied to the subscribers.

When the authentication server returns tunnel attributes, these returned values take precedence over the corresponding local tunnel configuration values in the AAA domain map. If the server does not return any tunnel attributes, then the tunnel subscriber's tunnel settings are configured according to the domain map's tunnel settings.

If the authentication server returns a redirect VSA and the corresponding AAA domain map has local tunnel configurations, the VSA is ignored. Access is denied to the user when the authentication server rejects the access request.

The **tunnel-subscriber authentication** command has no effect on subscribers in a domain with no tunnel configuration. When a AAA domain map has no tunnel configuration, subscribers in the domain are authenticated by the authentication server. If the server grants access, then the subscribers get their tunnel settings only from the authentication server.

By default, tunnel subscribers in the domain are granted access with no external authentication. Use the **enable** keyword to enable authentication. Use the **disable** keyword to restore disable user authentication.

To configure authentication of tunnel subscribers within a AAA domain by an external authentication server.

- Example

  host1(config-domain-map)#tunnel-subscriber authentication enable

Related Documentation

- Overview of Mapping a User Domain to a Virtual Router on page 7
- tunnel-subscriber authentication

CHAPTER 4

Understanding Address Servers Functions

Name Server Addresses Configuration Overview

You can assign IP or IPv6 addresses for DNS and IP addresses for WINS name servers. During setup negotiations between the router and remote PC clients using PPP (Internet Protocol Control Protocol [IPCP] specifically), the remote client may request the DNS and WINS server IP addresses. If the IP addresses passed to the router by the remote PC client are different from the ones configured on your router, the router returns the values that you configured as the correct values to the remote PC client. This behavior is controlled by the **ppp peer dns** and **ppp peer wins** interface commands.

If a PPP client request contains address values of 0.0.0.0 for the name servers, the router considers that the remote PC client is not configured and returns the configured values as the correct values to the remote PC client.

The DNS and WINS addresses are considered as part of the PPP user information. These addresses are provided to the PPP client as part of the IPCP negotiations between PPP peers. For details, see RFC 1877—PPP Internet Protocol Control Protocol Extensions for Name Server Addresses (December 1995).

NOTE: **All name server address parameters are defined in the context of a virtual router.**

Related Documentation

- ppp peer

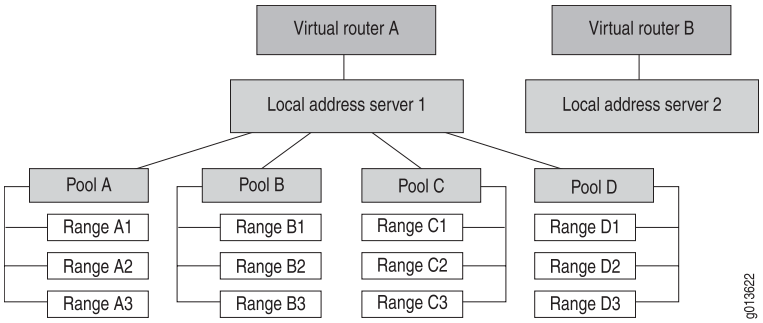
Local Address Servers Configuration Overview

The local address server allocates IP addresses from a pool of addresses stored locally on the router. You can optionally configure shared local address pools to obtain addresses from a DHCP local address pool that is in the same virtual router. Addresses are provided automatically to client sessions requiring an IP address from a virtual router that is configured to use a local address pool.

A local address server is defined in the context of a virtual router. You create a local address server when you configure the first local pool. Local address servers exist as long as the virtual router exists or until you remove them by deleting all configured pools.

Figure 1 on page 24 illustrates the local address pool hierarchy. Multiple local address server instances, one per virtual router. can exist. Each local address server can have one or more local address pools. Each pool can contain a number of IP addresses that are available for allocation and used by clients, such as PPP sessions.

Figure 1: Local Address Pool Hierarchy



The following sections describe local address servers:

- Local Address Pool Ranges on page 24
- Local Address Pool Aliases on page 24
- Shared Local Address Pools on page 25
- SNMP Thresholds on page 26

Local Address Pool Ranges

As shown in Figure 1 on page 24, each local address pool is named and contains ranges of sequentially ordered IP addresses. These addresses are allocated when the AAA server makes a request for an IP address.

If a local address pool range is exhausted, the next range of addresses is used. If all pool ranges are exhausted, you can configure a new range to extend or supplement the existing range of addresses, or you can create a new pool. The newly created pool range is then used for future address allocation. If addresses allocated from the first pool range are released, then subsequent requests for addresses are taken from the first pool range.

Addresses are assigned sequentially from a range within a pool. If a range has no addresses available, the next range within that pool is used. If a pool has no addresses available, the next configured pool is used, unless a specific pool is indicated.

Local Address Pool Aliases

An alias is an alternate name for an existing local address pool. It comprises an alias name and a pool name.

When the AAA server requests an IP address from a specific local address pool, the local address server first verifies whether an alias exists for the requested pool. If an alias exists,

the IP address is allocated from the pool specified by the alias. If no alias exists, the IP address is allocated from the pool originally specified in the request.

The use of aliases simplifies management of subscribers. For example, you can use an alias to migrate subscribers from one local address pool to another. Instead of having to modify countless subscriber records on the AAA server, you create an alias to make the configuration change.

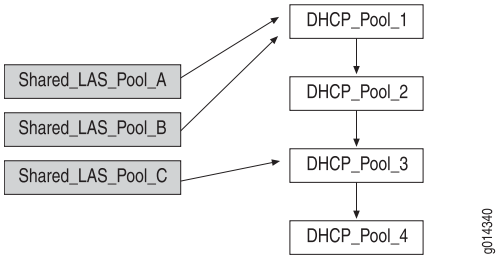
Shared Local Address Pools

Typically, the local address server allocates IP addresses from a pool of addresses that is stored locally on the router. However, *shared* local address pools enable a local address server to hand out addresses that are allocated from DHCP local server address pools within the same virtual router. The addresses are configured and managed within DHCP. Therefore, thresholds are not configured on the shared pool, but are instead managed by the referenced DHCP local server pool.

A shared local address pool references one DHCP address pool. The shared local address pool can then obtain addresses from the referenced DHCP address pool and from any DHCP address pools that are linked to the referenced DHCP address pool.

Figure 2 on page 25 illustrates a shared local address pool environment that includes four linked DHCP address pools. In the figure, both Shared_LAS_Pool_A and Shared_LAS_Pool_B reference DHCP_Pool_1, and can therefore obtain addresses from all four DHCP address pools. Shared_LAS_Pool_C references DHCP_Pool_3 and can get addresses from DHCP_Pool_3 and DHCP_Pool_4.

Figure 2: Shared Local Address Pools



When the local address server requests an address from a shared address pool, the address is returned from the referenced DHCP pool or a subsequent linked pool. If no address is available, DHCP notifies the local address server and the search is ended.

Keep the following guidelines in mind when using shared local address pools:

- The DHCP attributes do not apply to shared local address pools; for example, the lease time for shared local address pools is infinite.
- When you delete the referenced DHCP address pool, DHCP notifies the local address server and logs out all subscribers that are using addresses from the deleted pool.

- When you delete a shared local address pool, the local address server logs out the subscribers that are using addresses from the deleted pool, then notifies DHCP and releases the addresses.
- If the chain of linked DHCP address pools is broken, no action is taken and the existing subscribers retain their address. However, the DHCP local address pools that are no longer part of the chain are now unable to provide any new addresses.

The following commands create the shared address pools in Figure 2 on page 25:

```
host1(config)#ip local shared-pool Shared_LAS_Pool_A DHCP_Pool_1
host1(config)#ip local shared-pool Shared_LAS_Pool_B DHCP_Pool_1
host1(config)#ip local shared-pool Shared_LAS_Pool_C DHCP_Pool_3
```

SNMP Thresholds

A local address pool has SNMP thresholds associated with it that enable the local address server to signal SNMP traps when certain conditions exist. These thresholds include high utilization threshold and abated utilization threshold. If the outstanding addresses of a pool or a pool group exceed the high utilization threshold and the SNMP trap signaling is enabled, SNMP is notified. Likewise, when a pool's utilization drops below the abated utilization threshold, SNMP is notified.

A local address pool can be linked to a second local address pool so that when the first pool utilization reaches 100%, the DHCP local server uses the second pool. For generation of SNMP traps, the utilization of addresses is calculated for all the pools that are in the linked pools and they are collectively considered as an aggregated pool group.

Related Documentation

- Configuring a Local Address Server on page 105

CHAPTER 5

AAA Profiles

AAA Profile Configuration Overview

An AAA profile is a set of characteristics that act as a pattern that you can assign to domain names. Once you create an AAA profile, you can map it between a PPP client's domain name and certain AAA services on given interfaces. Using AAA profiles, you can:

- Allow or deny a domain name access to AAA authentication
- Map the original domain name to the mapped domain name for domain name lookup
- Use domain name aliases
- Force tunneling whenever a domain map contains tunnel attributes
- Manually set the NAS-Port-Type attribute (RADIUS attribute 61) for ATM and Ethernet interfaces
- Set the Service-Description attribute (RADIUS attribute 26-53)

An AAA profile contains a set of commands to control access for the incoming PPP subscriber. If no AAA profile is used, AAA continues as normal. The user's name and domain name are not changed as a result of an AAA profile mapping.

NOTE: There are two domain names with special meaning. The domain name **none** indicates that there is no domain name present in the subscriber's name. The domain name **default** indicates that no other match occurs.

Related Documentation

- Single Name Specification for Users from a Domain Overview
- Example: Configuring AAA Local Authentication on page 200

AAA Logical Line Identifier for Subscriber Tracking Overview

You can configure the router to support the AAA logical line identification feature. This feature enables service providers to track subscribers on the basis of a virtual port known as the logical line ID (LLID).

The LLID is an alphanumeric string that logically identifies a subscriber line. The service provider maps each subscriber to an LLID based on the user name and circuit ID from which the customer's calls originate. When a subscriber moves to a new physical line, the service provider's customer profile database is updated to map to the same LLID.

Because a subscriber's LLID remains the same regardless of the subscriber's physical location, using the LLID gives service providers a more secure mechanism for tracking subscribers and maintaining the customer database.

The following section explains how the router obtains and uses the LLID:

- How the Router Obtains and Uses the LLID on page 28

How the Router Obtains and Uses the LLID

To obtain an LLID for a subscriber, the router must issue two RADIUS access requests: a preauthentication request to obtain the LLID, followed by an authentication request encoded with the LLID returned in response to the preauthentication request.

To configure this feature, you:

1. Create an AAA profile that supports preauthentication (by using the **pre-authenticate** command in AAA Profile Configuration mode).
2. Specify the IP address of a RADIUS preauthentication server (by using the **radius pre-authentication server** command in Global Configuration mode) and of an authentication server (by using the **radius authentication server** command in Global Configuration mode).

The following steps describe how the router uses RADIUS to obtain and use the LLID. It is assumed that you have already configured an AAA profile for preauthentication and have defined both a RADIUS preauthentication server and a RADIUS authentication server. Typically, the preauthentication server and the authentication server reside in the same virtual router context in which the PPP subscriber is authenticated.

The router obtains and uses the LLID as follows:

1. A PPP subscriber requests authentication through RADIUS.
2. The router sends an Access-Request message to the RADIUS preauthentication server to obtain an LLID for the subscriber.

   This step is referred to as the preauthentication request because it occurs before user authentication and authorization.
3. The preauthentication server returns the LLID to the router in the Calling-Station-Id (RADIUS attribute 31) of an Access-Accept message.

The router ignores any RADIUS attributes other than the Calling-Station-Id that are returned in the preauthentication Access-Accept message.

4. The router encodes the LLID in the RADIUS Calling-Station-Id and sends an Access-Request message to the RADIUS authentication server.

   This step is referred to as the authentication request.

5. The RADIUS authentication server returns an Access-Accept message to the router that includes the tunnel attributes for the subscriber session.

6. For tunneled PPP subscribers, the router, acting as an L2TP access concentrator (LAC), encodes the LLID into L2TP Calling Number AVP 22 and sends this to the L2TP network server (LNS) in an incoming-call request (ICRQ) packet.

   After a successful preauthentication request, the router always encodes the LLID in Calling Number AVP 22. The use of **aaa** commands such as **aaa tunnel calling-number-format** to control or change the inclusion of the LLID in Calling Number AVP 22 has no effect.

Related Documentation

- Configuring RADIUS AAA Servers on page 95
- Configuring the Router to Obtain the LLID for a Subscriber on page 120

RADIUS Attributes in Preauthentication Request

Table 4 on page 29 describes the RADIUS IETF attributes that are always included in a preauthentication request to obtain the LLID. The attributes are listed in ascending order by standard number.

Table 4: RADIUS IETF Attributes in Preauthentication Request

Attribute Number	Attribute Name	Description
[1]	User-Name	Name of the user associated with the LLID, in the format: NAS-Port:<NAS-IP-Address>:<Nas-Port-Id> For example, nas-port:172.28.30.117:atm 4/1.104:2.104
[2]	User-Password	Password of the user to be authenticated; always set to “ juniper”
[4]	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user; for example, 172.28.30.117
[5]	NAS-Port	Physical port number of the NAS that is authenticating the user; this is always interpreted as a bit field
[6]	Service-Type	Type of service the user has requested or the type of service to be provided; for example, framed

Table 4: RADIUS IETF Attributes in Preauthentication Request *(continued)*

Attribute Number	Attribute Name	Description
[61]	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user
[77]	Connect-Info	Actual user name; for example, jdoe@xyzcorp.east.com
[87]	NAS-Port-Id	Text string that identifies the physical interface of the NAS that is authenticating the user; for example, atm 4/1.104:2.104

The use of **radius** commands such as **radius calling-station-format** or **radius override calling-station-id** to control or change the inclusion of these attributes in the preauthentication request has no effect.

Related Documentation

- RADIUS IETF Attributes
- Troubleshooting Subscriber Preauthentication on page 351

Considerations for Using the LLID

The following considerations apply when you configure the router for subscriber preauthentication:

- Only PPP subscribers authenticating through RADIUS can use the AAA LLID feature on the router. PPP subscribers tunneled through domain maps cannot take advantage of this feature.
- The Calling-Station-Id [31] attribute is typically sent in RADIUS Access-Request messages, not in Access-Accept messages as is the case for this feature. As a result, your RADIUS server might require special configuration procedures to enable the Calling-Station-Id attribute to be returned in Access-Accept messages. See the documentation that came with your RADIUS server for information.
- The router ignores any RADIUS attributes other than the Calling-Station-Id that are returned in the preauthentication Access-Accept message.
- If a preauthentication request fails due to misconfiguration of the preauthentication server, timeout of the preauthentication server, or rejection of the preauthentication request by the preauthentication server, the authentication process continues normally and the preauthentication request is ignored.
- The router preserves the LLID value for established subscribers after a stateful SRP switchover.
- The **radius rollover-on-reject enable** command has no effect for a RADIUS preauthentication server. That is, you cannot use the **radius rollover-on-reject enable** command to configure the router to roll over to the next RADIUS preauthentication

server when the router receives an Access-Reject message for the user it is authenticating.

Related Documentation

- Configuring RADIUS AAA Servers on page 95

CHAPTER 6

Route Download Servers for IPv4 and IPv6 Routes

RADIUS Route-Download Server for Route Distribution Overview

The JunosE RADIUS route-download server provides periodic automatic distribution of IPv4 and IPv6 access routes, which enables preconfiguration and preadvertising of access routes before they are assigned to clients. Using the route-download server helps eliminate routing protocol storms and other delays in client service activation that can be caused by protocol convergence or a large number of simultaneous customer activations.

The RADIUS route-download server periodically sends a RADIUS Access-Request message to the RADIUS server to request that routes be downloaded. The RADIUS server then responds with an Access-Accept message and downloads the configured routes. When the download operation is complete, the route-download server installs the access routes in the routing table.

JunosE Software supports the creation of one RADIUS route-download server per chassis.

Format of Downloaded Routes

The RADIUS server sends the downloaded routes to the RADIUS route-download server in the following format:

[{ vir | virtual-router } *virtualRouterName*] [vrf *vrfName*] prefix-mask [{ null0 | null 0 } [cost]] [tag *tagValue*]

For IPv4 routes, the route-download server accepts downloaded routes in either the Framed-Route attribute (RADIUS attribute 22) or the Cisco AV-pair attribute (Cisco VSA 26-1).

For IPv6 routes, the route-download server accepts downloaded routes in either the Framed-IPv6-Route attribute (RADIUS attribute 99) or the Cisco AV-pair attribute (Cisco VSA 26-1).

Framed-Route (RADIUS attribute 22)

NAS-1 Password = “14raddlsvr” User-Service-Type = Outbound-User
Framed-Route = “192.168.3.0 255.255.255.0 null0”
Framed-Route = “vrf vrfboston 192.168.1.0/24 null 0 0 tag 6”
Framed-Route = “vir host1 vrf vrfsunny 192.168.0.0/16 null0 0 tag 8”

Framed-IPv6-Route (RADIUS attribute 99)

NAS-1 Password = “14raddlsvr” User-Service-Type = Outbound-User
Framed-IPv6-Route = “2001:DB8:cc00:1::/48 null0"
Framed-IPv6-Route = “vrf test 2001:DB8:cc00:1::/48 null 0 0 tag 6"
Framed-IPv6-Route = "vir zzz vrf test1 2001:DB8:cc00:1::/48 null0 0 tag 8”

Cisco AV-Pair (Cisco VSA 26-1)

- NAS-1 Password = “14raddlsvr” User-Service-Type = Outbound-User
  cisco-avpair = “ip:route = 192.168.3.0 255.255.255.0 null0”
  cisco-avpair = “ip:route = vrf vrfboston 192.168.1.0/24 null 0 0 tag 6”
  cisco-avpair = “ip:route = vir host1 vrf vrfsunny 192.168.0.0/16 null0 0 tag 8”
- NAS-1 Password = “14raddlsvr” User-Service-Type = Outbound-User
  cisco-avpair = "ipv6:route=2001:DB8:cc00:1::/48 null0"
  cisco-avpair = "ipv6:route=vrf test 2001:DB8:cc00:1::/48 null 0 0 tag 6"
  cisco-avpair = "ipv6:route=vir zzz vrf test1 2001:DB8:cc00:1::/48 null0 0 tag 8”

NOTE: The prefix-mask entry in downloaded routes can be in the form of prefix length, prefix mask, or prefix. If prefix is used, the mask is determined by the IP address class of the prefix.

How the Route-Download Server Downloads Routes

The route-download server starts the initial route-download operation (for example, after a system reboot or the first time the route-download server is enabled) as soon as IP is established in the virtual router in which the download is performed. After the initial route-download process is established, the router repeats the route download operation based on either the default download schedule or the schedule you specify. You can also initiate an immediate route download at any time.

The RADIUS route-download server downloads routes in two stages—first, all routes are downloaded from the RADIUS server to the router’s download database and examined for errors. Next, the router updates the routing table with the new routes, using the following guidelines:

- Adds all downloaded routes that are not already installed in the routing table
- Does not add downloaded routes that are already installed in the routing table
- Deletes routes from the routing table that do not appear in the newly downloaded group

Related Documentation

- Configuring RADIUS AAA Servers on page 95
- Configuring the Route-Download Server to Download Routes on page 123

CHAPTER 7

Termination of PPP and L2TP Subscriber Sessions

Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes

The JunosE Software uses a default configuration that maps terminate reasons to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute—these mappings enable you to provide different information about the cause of a termination.

When a subscriber's 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.

Use the **show terminate-code** command to display information about the mappings between application terminate reasons and RADIUS Acct-Terminate-Cause attributes.

Table 5 on page 37 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 5: 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

Table 5: Supported RADIUS Acct-Terminate-Cause Codes *(continued)*

Code	Name	Description
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
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 Mappings for PPP Terminate Reasons

Timeout Configuration Overview

You can configure an idle timeout or a session timeout. The values you set are the default values for Point-to-Point Protocol Broadband Remote Access Server users. Attributes returned by RADIUS override these default settings on a per-user basis.

When you set an idle timeout, the PPP application on the router monitors both ingress (inbound) traffic and egress (outbound) traffic by default for the configured idle timeout period to determine whether to disconnect an inactive PPP session. If there is no activity in either direction on the interfaces for more than the configured idle timeout period, the router terminates the PPP session.

You can optionally configure the router to monitor only ingress traffic for the configured idle timeout period to determine session inactivity and subsequent disconnection of an inactive PPP session. Monitoring only ingress traffic for the idle timeout is useful for networks in which the PPP keepalive timer is disabled for wireless subscribers. Without the keepalive timer, the router cannot detect whether a wireless subscriber has been disconnected. Monitoring egress traffic does not indicate inactivity for wireless subscribers because egress traffic is always flowing. Enabling the router to monitor only ingress traffic enables you to selectively disconnect subscribers, including wireless subscribers, if no traffic is received for the configured idle timeout period.

If you do not configure a session timeout, or you set its value to 0, the session remains active for an infinite lifetime. You can use the **show ppp session-To-Thirteen-Years** command along with **show ppp interface full** in Privileged Exec or User Exec mode to verify whether the capability to preserve PPP sessions for a timeout duration of 13 years is enabled. If the **show ppp session-To-Thirteen-Years** command is not executed, the session timeout value is set to the maximum session timeout value of 366 days.

If the RADIUS server returns the value 0 for the Session-Timeout attribute, then the session remains active for an infinite lifetime even if a value is configured through the CLI.

The following sections describe timeout configuration:

- Limiting Active Subscribers on page 39
- AAA Failure Notification for RADIUS on page 39
- Configuring AAA Session Timeout on page 40

Limiting Active Subscribers

You can limit the number of active subscribers on a port or virtual router.

AAA Failure Notification for RADIUS

If a user passes RADIUS authentication, but fails AAA authentication, the RADIUS server may still allocate an address for the user from its internal address pool. To indicate to the RADIUS server to free the address, you can set up the router to send an Acct-Stop message if a user fails AAA.

Configuring AAA Session Timeout

You can use the **aaa timeout session *sessionTimeout*** command to configure a session timeout. Restoring the session timeout to the default value causes the PPP B-RAS session to remain active for an infinite lifetime.

Related Documentation

- Configuring RADIUS AAA Servers on page 95
- Configuring Custom Mappings for PPP Terminate Reasons

CHAPTER 8

DHCPv6 Prefix Delegation and IPv6 Neighbor Discovery for AAA Subscribers

Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration

When an E Series router is configured for IP version 6, it uses router advertisements to announce its presence to other nodes connected to it. Hosts discover the addresses of their neighboring routers by listening for these advertisements. When the routing protocol process first starts on the server router, the server sends router advertisement packets every few seconds. Then, the server sends these packets less frequently. The server responds to route solicitation packets it receives from a client. The response is sent unicast, unless a router advertisement packet is due to be sent out momentarily. IPv6 supports the following router advertisement mechanisms:

- ICMPv6 Neighbor Discovery router advertisements
- DHCPv6 Prefix Delegation
- ICMPv6 Neighbor Discovery router advertisements followed by DHCPv6 Prefix Delegation

The AAA service on the router stores the prefixes that it receives from the RADIUS server during the PPPv6 authentication phase. After the PPPv6 link is established between the subscriber and the B-RAS application running on the router, the router receives the ICMPv6 router solicitation message, the DHCPv6 Solicit message, or both of them based on the prefix advertisement mechanism. In previous releases, you were not able to configure the RADIUS attribute or VSA to be used for IPv6 Neighbor Discovery router advertisements

and DHCPv6 Prefix Delegation through the CLI. As a result, the IPv6-NdRa-Prefix attribute returned in the Access-Accept message was used for IPv6 Neighbor Discovery router advertisements and the Framed-IPv6-Prefix RADIUS attribute in the Access-Accept message was used for DHCPv6 Prefix Delegation.

In this release, you can control the RADIUS IETF attribute or VSA to be used for IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation by using **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** and **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** commands, respectively, in Global Configuration mode on each virtual router.

Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHPCv6 Local Server and Neighbor Discovery Router Advertisements

When both IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation methods are used to assign IPv6 prefixes to clients, either two or three host routes for IPv6 might be consumed from the routing table depending on the way in which the router advertisement prefix is determined. The following sections describe sample configuration scenarios to illustrate how a maximum of 48,000 subscribers can be handled for delegation of IPv6 prefixes, based on whether a unique IPv6 prefix is allocated to a client or the same IPv6 prefix is allocated to multiple clients:

- Delegation of a Unique IPv6 Prefix per Subscriber Example on page 42
- Delegation of the Same IPv6 Prefix for Multiple Subscribers Example on page 43

Delegation of a Unique IPv6 Prefix per Subscriber Example

Consider a scenario in which the RADIUS server is configured to assign a unique router advertisement prefix route to each IPv6 subscriber. In such a case, two routes are used for Neighbor Discovery and one IPv6 route is consumed for Prefix Delegation, which results in a total of three routes being utilized for each subscriber. If such a method for allocating prefixes to subscribers is configured, approximately 33,333 IPv6 bindings can be supported before the maximum IPv6 static route limit of 100,000 routes is reached. Therefore, in such a deployment, it is not possible to handle 48,000 subscribers for delegation of IPv6 prefixes using the DHCPv6 local server Prefix Delegation and Neighbor Discovery methods.

The following output of the **show ipv6 route** command displays how three routes are used by the same subscriber, as can be seen from the Interface field in the output. The routes are assigned using Prefix Delegation, Neighbor Discovery, and the access-internal route, such as the DHCP and AAA/PPP host route, which is a host route to directly connected clients. Access routes, also known as AAA framed routes, are sourced by AAA.

```
host1#show ipv6 route

Prefix/Length                      Type      Dst/Met     Interface
---------------------------------  ---------  --------   ----------------
1111:1111:1111:1111::/64           Access     3/0        GigabitEthernet0/2.600.6
1111:1111:2222:2222::/64           AccIntern  2/0        GigabitEthernet0/2.600.6
1111:1111:2222:2222:21b:c0ff:fe4   AccIntern  2/0        GigabitEthernet0/2.600.6 b:9d00/128
```

Delegation of the Same IPv6 Prefix for Multiple Subscribers Example

Consider a scenario in which the same prefix with a length of /64 for ICMPv6 Neighbor Discovery router advertisements is assigned to all subscribers by configuring the prefix in the profile or by configuring the RADIUS server to send the same prefix in the Framed-IPv6-Prefix attribute (RADIUS IETF attribute 97) of the RADIUS-Access-Accept message. In such a topology, a unique /64 IPv6 route is not present per subscriber. Instead, one /64 prefix with multiple next-hops is assigned for all the subscribers.

If you use this method for allocating IPv6 prefixes of /64 length to subscribers, Neighbor Discovery consumes one IPv6 route and Prefix Delegation consumes one IPv6 route, which results in a total of two IPv6 routes per subscriber being used. Therefore, it is possible to scale up to a maximum of 48,000 subscribers for delegation of IPv6 prefixes.

The increased scaling limit of support for delegation of IPv6 prefixes using the DHCPv6 local server Prefix Delegation mechanism for 48,000 subscribers applies only to E120 and E320 routers and not to ERX14xx models, ERX7xx models, and the ERX310 router because the binding information is stored in the SRP modules of E120 and E320 routers. Also, a limitation exists on the number of IPv6 interfaces and the IPv6 routing table size supported by ERX routers that prevents the support for 48,000 subscribers for Prefix Delegation on DHCPv6 local servers running on those routers.

To enable support for 48,000 subscribers for IPv6 Prefix Delegation, about 5.5 MB of memory on the SRP module is consumed additionally.

Related Documentation

- Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server on page 43

Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server

IPv6 prefixes are delegated to subscribers using two mechanisms: ICMPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation. When the router receives the ICMPv6 router solicitation message, the DHCPv6 Solicit message, or both the messages based on the prefix advertisement mechanism, a prefix is assigned to the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client. Consider a scenario in which the CPE device uses the Prefix Delegation feature alone to obtain IPv6 prefixes from the delegating router, which is the DHCPv6 local server. Also, assume that IPv6 Neighbor Discovery is not configured for allocation of prefixes to the client. In such an environment, each IPv6 subscriber uses only a single route entry and the maximum number of subscribers to which IPv6 prefixes can be delegated from the DHCPv6 local server is 48,000.

Related Documentation

- Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHPCv6 Local Server and Neighbor Discovery Router Advertisements on page 42

DHCPv6 Local Address Pools for Allocation of IPv6 Prefixes Overview

In previous releases, you configured DHCPv6 local servers on a virtual router to delegate IPv6 prefixes to DHCPv6 clients. In this release, you can configure IPv6 local address pools to allocate IPv6 prefixes to clients in networks that use DHCPv6. These pools can be used to assign prefixes from a delegating router, which is an E Series router configured as a DHCPv6 local server, to the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client.

The DHCPv6 prefix delegation feature is useful in scenarios in which the delegating router does not have information about the topology of the networks in which the customer edge device or requesting router is located. In such cases, the delegating router requires only the identity of the requesting router to choose a prefix for delegation. An IPv6 local pool is configured on the delegating router, which contains information about the prefixes, their validity periods, and other parameters to control their assignment to the requesting routers. The delegating router is configured with a set of prefixes that is used to assign to a CPE or DHCPv6 client, when it first establishes a connection with an Internet service provider (ISP).

When the delegating router receives a request from a DHCPv6 client, it selects an available prefix and delegates it to the client. The DHCPv6 client subnets the delegated prefix and assigns the prefixes to links at the customer edge.

Keep the following points in mind when you configure IPv6 local address pools to assign prefixes to requesting routers:

- You must enable the IPv6 local address pool feature to be able to configure IPv6 local address pools.
- You can configure IPv6 local address pools for DHCP to allocate prefixes to client requests that are received over PPP or non-PPP links, such as VLAN, S-VLAN, or Ethernet.
- You can configure multiple local address pools on a single virtual router, up to a maximum of 500 pools per virtual router.
- You can also configure multiple address pools on multiple virtual routers. Each IPv6 local address pool must have a unique name.
- You can configure a valid and preferred lifetime for each IPv6 prefix, which determines the length of time the requesting router can use the prefix.
- You can configure multiple prefix ranges in an IPv6 local pool. The ranges can have the same or different assigned prefix lengths.
- You cannot configure overlapping prefix ranges in an IPv6 local pool. If you try to configure a prefix range that overlaps with an existing prefix range in the IPv6 local pool, an error message is displayed stating that the prefix range could not be configured. Similarly, an error message is displayed if you try to configure a prefix range in an IPv6 local pool that overlaps with a prefix range in another IPv6 local pool on the same virtual router.

- You can configure certain prefix ranges to be excluded from being used for delegation to the requesting router.
- You can configure the IPv6 addresses of a primary and secondary DNS server in an IPv6 local pool. The DNS server addresses are returned to the client in DHCPv6 responses as part of the DNS Recursive Name Server option.
- You can configure a list of up to four domain names in an IPv6 local pool to be used during the resolution of hostnames to IP addresses. These domain names are returned to clients in the DHCPv6 responses as part of the Domain Search List option.
- You can configure an IPv6 local address pool in an AAA domain map to assign prefixes to requesting DHCPv6 clients using the **ipv6 prefix-pool-name** command in Domain Map Configuration mode. If the authentication server returns the IPv6 local address pool name in the Framed-IPv6-Pool attribute of the RADIUS-Access-Accept message, this pool overrides the IPv6 local address pool configured in the domain map.
- You cannot delete a pool or a prefix range from which prefixes have been allocated to requesting routers or DHCPv6 clients. However, you can forcibly delete such a pool or prefix range by using the **force** keyword in the **ipv6 local pool** *poolName* and **prefix** commands. If a pool is deleted or the prefix range associated with the pool is deleted, and prefixes have been assigned to DHCPv6 clients or requesting routers, the corresponding DHCPv6 bindings are also deleted.
- When multiple prefix ranges are configured in a pool, the DHCPv6 prefix delegation feature allocates prefixes from the configured ranges in the order of the assigned prefix length. The delegating router or the DHCv6 server attempts to allocate a prefix from the range with lowest assigned prefix length. If this attempt fails because the pool has been fully allocated, the server tries to allocate a prefix from the subsequent prefix ranges. These ranges could have the same prefix length as the first one or a higher length.

  NOTE: Although you can configure an IPv6 local pool with the assigned prefix length as /128, which implies a full IPv6 address, this assignment is not useful for the DHCPv6 prefix delegation feature because it assigns a prefix with a length of only /64 or less. A pool with an assigned prefix length of /128 is useful when complete IPv6 addresses are assigned to the DHCPv6 clients.

- When an IPv6 client that is connected to the requesting router using a PPP link is delegated a prefix by the DHCPv6 server, the client binding is removed when the PPP interface goes down and is not retained until the lease time expires. A new client binding is created for the PPP subscriber in response to a renew or rebind request sent to the DHCP server. This method of re-creating the client binding ensures that the client receives a new authentication configuration and is assigned a prefix when it sends a rebind or renew request after the PPP interface flaps (constantly goes up and down).

When a PPP user establishes a PPP connection with the E Series router functioning as a remote access server, the subscriber is first authenticated using the RADIUS protocol. The Access-Accept message returned from the RADIUS server can contain different IPv6 attributes, including the Framed-IPv6-Pool attribute, which contains the name of the

IPv6 pool from which a prefix needs to be assigned to the subscriber. The prefix is assigned to the subscriber using the DHCPv6 prefix delegation feature, which is covered in the next section.

Related Documentation

- Example: Delegating the DHCPv6 Prefix on page 198

IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview

You can configure IPv6 local address pools for Neighbor Discovery router advertisements on a virtual router in order to allocate prefixes to Neighbor Discovery clients. These pools can be used to assign prefixes from the E Series router.

An IPv6 local address pool for Neighbor Discovery router advertisements is configured on the router running the B-RAS application, which contains information about the prefixes. When the B-RAS application running on the E Series router receives a request from a PPP IPv6 client, it selects an available prefix and allocates it to the client.

Allocation of Neighbor Discovery Prefixes for IPv6 Subscribers over PPP Links

When a PPP user establishes a PPP connection with the E Series router functioning as a remote access server, the subscriber is first authenticated using the RADIUS protocol. The Access-Accept message returned from the RADIUS server can contain different IPv6 attributes, including the IPv6-NdRa-Pool attribute, which contains the name of the IPv6 pool from which a prefix needs to be assigned to the subscriber. The prefix is assigned to the subscriber using the Neighbor Discovery router advertisements feature.

Order of Preference in Determining the Local Address Pool for Allocating Prefixes for Neighbor Discovery Router Advertisements

You can configure multiple local address pools for Neighbor Discovery router advertisements on a virtual router. When multiple pools are configured, the pool that is used to allocate the prefix to the requesting PPPv6 subscriber is selected using the following order of preference:

1. If the **aaa dhcpv6-ndra-pool override** command is not configured and a pool name is returned by the RADIUS server in the IPv6-Ndra-Pool attribute, that pool is used to allocate the prefix to the client.
2. If the **aaa dhcpv6-ndra-pool override** command is configured and a pool name is returned by the RADIUS server in the Framed-Ipv6-Pool attribute, that pool is used to allocate the prefix to the client.
3. If the RADIUS server does not return a pool name in either of the above-mentioned points, based on the **aaa dhcpv6-ndra-pool override** command, the pool name configured in the AAA domain map is used.

Order of Preference in Assigning Prefixes when Neighbor Discovery Router Advertisements are Configured on an Interface

The router running the B-RAS application uses the following order of preference to determine the source from which the Neighbor Discovery router advertisements prefix is allocated to the requesting PPPv6 subscriber from the Neighbor Discovery Router Advertisements server:

1. An interface that is configured for the Neighbor Discovery router advertisements prefix is given priority over the RADIUS attributes returned in the Access-Accept message or the prefixes configured in the IPv6 local address pool for Neighbor Discovery router advertisements on the router running the B-RAS application.
2. The RADIUS server might return one or more of the following attributes in the Access-Accept message in response to the client authentication request:
   - Ipv6-NdRa-Prefix (VSA 26-129)
   - Framed-IPv6-Prefix (RADIUS IETF attribute 97)
   - Framed-IPv6-Pool (RADIUS IETF attribute 100)
   - IPv6-Ndra-Pool (VSA 26-157)

   If either of the first two attributes are returned, then the prefix contained in those attributes is used, and the pool name in the Framed-IPv6-Pool or Ipv6-Ndra-Pool attribute is ignored.
3. If the RADIUS server does not return any of the above-mentioned attributes, the IPv6 prefix pool name of the Neighbor Discovery router advertisements mentioned in the AAA domain map will be used to allocate the prefix to the requesting PPPv6 subscriber.

Guidelines for Allocating Neighbor Discovery Prefixes Using IPv6 Address Pools

The following are guidelines for allocating prefixes using IPv6 address pools for Neighbor Discovery router advertisements:

- You must enable the IPv6 local address pool for the Neighbor Discovery router advertisements feature to be able to configure IPv6 local address pools for Neighbor Discovery router advertisements.
- You can configure IPv6 local address pools for Neighbor Discovery router advertisements to allocate prefixes to client requests that are received over PPP.
- You can configure multiple local address pools on a single virtual router up to a maximum of 500 pools per virtual router.
- You can also configure multiple address pools on multiple virtual routers. Each IPv6 local address pool must have a unique name.
- You can configure up to ten prefix ranges in an IPv6 local address pool. The ranges can have only /64 prefix length.
- You can configure a maximum of 1,048,576 prefixes per prefix range to be used for allocation of prefixes to clients using Neighbor Discovery router advertisements. If you

attempt to configure prefixes after the maximum limit of prefixes per prefix range is exceeded, a warning message stating that automatic truncation will be performed is displayed.

- You can configure a maximum of 400,000,000 prefixes throughout the system for allocation of prefixes using Neighbor Discovery router advertisements. An error message is displayed if you attempt to configure a prefix for a pool when this maximum system-wide limit is exceeded.
- If you configure the maximum number of IPv6 prefixes, which is 1,048,576 per prefix range, for the first 383 local address pools for Neighbor Discovery router advertisements by using the **ipv6 local ndra-pool** *poolName* command, the system-wide maximum limitation of 400,000,000 is reached. In such a case, if you attempt to configure the IPv6 prefix ranges to be allocated for the 384th pool, an error message is displayed stating that the prefix cannot be configured. Although all of the 500 IPv6 local address pools are configured correctly, you cannot configure prefixes for Neighbor Discovery from the 384th pool through the 500th pool because the maximum number of prefixes supported for the entire system is reached with the 383rd pool.
- You cannot configure overlapping prefix ranges in an IPv6 local pool. If you try to configure a prefix range that overlaps with an existing prefix range in the IPv6 local pool, an error message is displayed stating that the prefix range could not be configured. Similarly, an error message is displayed if you try to configure a prefix range in an IPv6 local pool that overlaps with a prefix range in another IPv6 local pool on the same virtual router.
- You can configure certain prefix ranges to be excluded from being used for allocation to the requesting subscriber.
- You can configure the name of an IPv6 local address pool in an AAA domain map using the **ipv6-ndra-pool-name** command in Domain Map Configuration mode. If the authentication server returns the IPv6 local address pool name in the Framed-IPv6-Pool attribute or Ipv6-NdRa-Pool attribute of the RADIUS-Access-Accept message, this pool overrides the IPv6 local address pool configured in the domain map.
- You cannot delete a pool or a prefix range from which prefixes have been allocated to requesting routers or Neighbor Discovery router advertisements clients. However, you can forcibly delete such a pool or prefix range by using the **force** keyword in the **ipv6 local ndra-pool** *poolName* and **ndraprefix** commands. If a pool is deleted or the prefix range associated with the pool is deleted forcibly, corresponding subscribers will be logged out forcibly.
- Two new RADIUS attributes are added: Ipv6-Ndra-Pool and Delegated-Ipv6-Pool. For more information on these attributes see Juniper Networks VSAs.
- You can issue the **aaa dhcpv6-ndra-pool override** command to use Framed-Ipv6-Pool attribute for IPv6 Neighbor Discovery router advertisements and the Delegated-Ipv6-Pool attribute for DHCPv6 Prefix Delegation. The **no** version of this command causes the Ipv6-NdRa-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Framed-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation.
- If you want the IPv6-NdRa-Prefix attribute to be included in the Acct-Start messages that the router sends to the RADIUS server, you can use the **radius include**

ipv6-ndra-prefix acct-start enable command. In such a case, the prefix allocated to the subscriber from the IPv6 local address pool for Neighbor Discovery is included in the Ipv6-NdRa-Prefix attribute or the Framed-Ipv6-Prefix attribute.

Similarly, to cause the Ipv6-NdRa-Prefix attribute to be included in the Acct-Stop messages sent to the RADIUS server, you can use the **radius include ipv6-ndra-prefix acct-stop enable** command. You can use the **disable** keyword with the **radius include ipv6-ndra-prefix acct-start** and **radius include ipv6-ndra-prefix acct-stop** commands to prevent the Ipv6-NdRa-Prefix attribute to be sent in the Acct-Start or Acct-Stop messages.

Related Documentation

- Configuring the DHCPv6 Local Address Pools on page 106
- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108
- aaa dhcpv6-ndra-pool override on page 134
- ipv6 address-pool ndra on page 161
- ipv6 local ndra-pool on page 162

CHAPTER 9

Validation of Duplicate Prefixes and Addresses

Duplicate IPv6 Prefix Check Overview

You can configure AAA service to detect duplicates of IPv6 Neighbor Discovery router advertisement prefixes and DHCPv6 delegated prefixes. If a non-unique IPv6 prefix is detected by AAA, the subscriber session corresponding to the duplicate prefix is terminated.

In some network environments where the same customer logs in from multiple locations, terminating sessions with duplicate IPv6 prefixes might result in breaking subscriber setup. The duplicate IPv6 prefix-check capability is disabled by default.

If a duplicate prefix is detected by AAA before a subscriber is granted access, the subscriber is denied access. However in some cases, when two subscribers having the same IPv6 prefix log in simultaneously, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate IPv6 prefix.

NOTE: **AAA cannot detect duplicates of overlapping IPv6 prefixes.**

Related Documentation

- Configuring Duplicate IPv6 Prefix Check on page 127
- Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration on page 41

Duplicate IPv6 Prefix Detection in the AAA User Profile Database Overview

You can configure AAA service to detect duplicates of both IP and IPv6 Neighbor Discovery router advertisement prefixes, Framed-IPv6-Prefixes, and DHCPv6 delegated prefixes by validating the prefixes against the AAA database instead of the IP route table. If AAA

detects a non-unique IP address or IPv6 prefix, the corresponding subscriber session is terminated.

In some network environments where the same customer logs in from multiple locations, terminating sessions with duplicate IP addresses and IPv6 prefixes might result in breaking subscriber setup. The enhanced duplicate prefix detection capability is disabled by default. Because the prefix is validated against the AAA table, enabling the enhanced prefix detection capability may impact performance.

AAA maintains a new table for IPv6 prefixes and Framed-IP-Address information for subscribers. The AAA service checks for duplication of IP addresses and prefixes in this new table after PPP authorization. If a duplicate address or prefix is detected by AAA before a subscriber is granted access, the subscriber is denied access. However, in some cases, when two subscribers with the same IPv6 prefix log in simultaneously, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate IPv6 prefix.

The following scenarios can occur during the establishment of subscriber sessions:

- When the RADIUS server assigns the same IPv6-NdRa-Prefix or Delegated-IPv6-Prefix to two subscribers, the second subscriber that contains the same prefix as the first subscriber is disconnected.
- When the RADIUS server assigns the same Framed-IPv6-Prefix to two dual-stack subscribers, the second subscriber session is rejected.
- When the RADIUS server assigns the same Framed-IP-Address and different IPv6 prefixes to two subscribers, the second subscriber session is terminated.

NOTE: **AAA cannot detect duplicates of overlapping IPv6 prefixes. Also, the aaa duplicate-prefix-check-extension command detects duplicate prefixes globally for all VRs and is not limited to detecting duplicates on a per-VR basis.**

Related Documentation

- Configuring Detection of Duplicate IPv6 Prefixes in the AAA User Profile Database on page 127
- Monitoring Duplicate IPv6 Prefixes in the AAA User Profile Database
- Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration on page 41
- **aaa duplicate-prefix-check-extension on page 145**
- **show aaa duplicate-prefix-check-extension on page 307**

Guidelines for Duplicate Address Verification

In dual-stack networks in which both IPv4 and IPv6 subscribers are available, the subscribers might be granted the same IPv4 and IPv6 addresses if one user logs in quickly

after another user has logged in. To avoid the problem of two sessions containing the same address, when you enable detection of duplicate addresses, the subscriber is completely terminated when a duplicate IPv4 or IPv6 address is detected. The duplicate check operation is performed for 32-bit IPv4 subnet masks and IPv6 addresses with a prefix length of 128.

The value of the Framed-IPv6-Address attribute is determined using the Framed-IPv6-Prefix and Framed-Interface-Id attributes, normally obtained from the MAC addresses of clients in the PPP Network Control Protocol (NCP) phase in the PPP link connection process. Because the Framed-IPv6-Address attribute is not available to AAA during the authentication phase (before NCP negotiation occurs), the duplicate address detection mechanism performed for IPv4 cannot be adopted for IPv6. To achieve this functionality, if IPv6 detects a duplicate address while adding the route, it notifies AAA about the duplicate and AAA terminates the subscriber.

To correctly enable duplicate address detection when subscribers log in simultaneously, the IP and AAA applications examine the access-route table instead of the route table. In certain scenarios, AAA cannot detect whether a subscriber requesting access uses the same address as another subscriber. When the IP application detects a duplicate address while adding the route, the IP application notifies AAA about the duplication to terminate the connection for that subscriber.

In certain cases, when two subscribers with the same address attempt to log in, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate address.

If AAA cannot determine the virtual router (VR) context configured in the profile during subscriber authentication, the subscriber that uses the same address as another subscriber is terminated immediately after the IP application detects the duplicate address. Such a disconnection of subscribers occurs even if the duplicate subscriber was granted access previously when the VR context was not available to AAA for processing.

In a dual-stack environment in which both IPv4 and IPv6 subscribers are present, if a subscriber that uses a duplicate IPv6 address is detected, the subscriber is denied access even if the IPv4 interface address is unique. This method of terminating subscriber sessions occurs to avoid duplicate sessions from being established in scenarios in which the IPv6 interface address is the same as another client, whereas the IPv4 interface address is unique.

The following scenarios can occur during the establishment of subscriber sessions in a dual-stack network in which clients using both IPv4 and IPv6 protocols are present, and when detection of duplicate addresses is enabled on the router that delegates addresses to requesting clients. These scenarios assume that the RADIUS server is configured on a VR other than the default VR and that the AAA domain name is mapped to a non-default VR.

- When the VR context for subscribers is configured in the AAA domain map or obtained from the RADIUS server, and the same IP address is returned for two dual-stack subscribers from the RADIUS server, only the first subscriber session is configured and the second client session is terminated.
- When the same IP address is returned from the RADIUS server or the domain map for two dual-stack subscribers that log in simultaneously, only the first subscriber session is established and the second subscriber that contains the same address or prefix as the first subscriber is disconnected. Termination of the second subscriber occurs even if detection of the duplicate address occurs only after access is granted.
- When the VR context for subscribers is configured in the AAA profile, and the same IP address is returned from the RADIUS server or the domain map for two dual-stack subscribers, only the first subscriber session is configured and the second client session is terminated.
- If you disable the routing table address lookup for duplicate addresses by using the **no aaa duplicate-address-check** command, define the VR context for subscribers in the profile, and the same address is returned for two dual-stack subscribers, both the subscriber sessions are brought up successfully. However, for the second subscriber, which contains the same address as the first client, only the IPv6 interface is enabled and the IPv4 interface is not brought up.
- If the same IPv6-NdRa-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, and the VR context for the subscribers is specified in the profile, only the first subscriber is brought up and the second subscriber session is rejected.
- If you set the Framed-IPv6-Prefix RADIUS attribute for IPv6 Neighbor Discovery router advertisements by using the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command, the same Framed-IPv6-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, and the VR context for the subscribers is specified in the profile or the domain map, only the first subscriber is brought up and the second subscriber session is rejected.
- If you set the Framed-IPv6-Prefix RADIUS attribute for IPv6 Neighbor Discovery router advertisements by using the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command, disable the routing table address lookup for duplicate addresses, specify the VR context for subscribers in the domain map, and the same Framed-IPv6-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, only the first subscriber is brought up and the second subscriber session is rejected.

Related Documentation

- Configuring Duplicate IPv6 Prefix Check on page 127

CHAPTER 10

Interoperation with SRC Software

SRC Client Configuration Overview

The JunosE Software has an embedded client that interacts with the Juniper Networks Session and Resource Control (SRC) software, enabling the SRC software to manage the router's policy and QoS configuration.

The connection between the router and the SRC software uses the Common Open Policy Service (COPS) protocol and is fully compliant with the COPS usage for policy provisioning (COPS-PR) specification. The router's SRC client functions as the COPS client, or policy enforcement point (PEP). The SRC software functions as the COPS server, or policy decision point (PDP).

Rate limiters are aggregated for dual-stack subscribers (IPv4 and IPv6) managed by the SRC software, using external parent groups and hierarchical policy parameters. The external parent groups and policy parameters are pushed to lower interfaces from the SRC software through the Siemens Selection Switch or Service Selection Center client.

NOTE: **You cannot override aggregation node values while attaching policies to the interface.**

Related Documentation

- Configuring the SRC Client on page 129

SRC Client and COPS Terminology

Table 6 on page 56 provides common terms used in the COPS environment.

Table 6: SRC Client and COPS Terminology

Term	Description
COPS	Common Open Policy Service; query-and-response protocol used to exchange policy information between a policy server and its clients.
COPS-PR	COPS usage for policy provisioning; the PEP requests policy provisioning when the operational state of interface and DHCP addresses changes.
PDP	Policy decision point; the COPS server. which makes policy decisions for itself and for clients that request decisions. The SRC software is the PDP.
PEP	Policy enforcement point; the COPS client, which enforces policy decisions. The JunosE COPS interface is a PEP.
PIB	Policy Information Base; a collection of sets of attributes that represent configuration information for a device.
SRC	Session and Resource Control (SRC) software, formerly the Service Deployment System (SDX) software; functions as a COPS PDP.

The JunosE Software COPS-PR implementation uses the outsourcing model that is described in RFC 3084. In this model, the PEP delegates responsibility to the PDP to make provisioning decisions on the PEP's behalf.

NOTE: When you upgrade from an earlier JunosE release, the software removes the instance of SSCC that was configured with XDR.

If you are going to perform a unified ISSU from a JunosE release numbered lower than Release 10.0.0 and you have an XDR configuration, unified ISSU is not supported while an XDR configuration is presented.

The provisioning is event-driven and is based on policy requests rather than on an action taken by an administrator—the provisioning is initiated when the PDP receives external requests and PEP events. Provisioning can be performed in bulk (for example, an entire QoS configuration) or in smaller segments (for example, updating a marking filter). The following list shows the interaction between the PEP and the PDP during the COPS-PR operation.

1. Initial connection
   a. PEP starts the COPS-PR connection with the PDP.
   b. PDP requests synchronization.
   c. PEP sends all currently provisioned policies to PDP.
2. Change of interface state
   a. PEP requests provisioning of an interface from the PDP.
   b. PDP determines policies and sends provisioning data to the PEP.

c. PEP provisions the policies.

3. PDP requests policy provisioning

   a. PDP determines new policies and sends provisioning data to the PEP.

   b. PEP provisions the policies.

The information exchange between the PDP and PEP consists of data that is modeled in Policy Information Bases (PIBs) and is encoded using the standard ASN.1 basic encoding rules (BERs).

JunosE Software uses the following PIBs:

Proprietary PIB

- JunosE-IP-PIB—This PIB defines the data model for manipulating IP service policies and addresses offered through DHCP in JunosE Software.

Non-proprietary PIBs

- COPS-PR-SPPI
- COPS-PR-SPPI-TC
- DIFFSERV-PIB
- FRAMEWORK-FEEDBACK-PIB
- FRAMEWORK-PIB
- FRAMEWORK-TC-PIB

The COPS-PR support in JunosE Software uses the proprietary PIB. This PIB consists of a series of tables that is supported in previous JunosE Software releases, including the proprietary accounting and address assignment mechanisms.

You can force the router to restart a COPS connection to, and resynchronize with, a PDP, without disabling the SRC client's COPS support. The SRC software and the SRC client maintain common state information in PIBs that both the SRC software and the SRC client use. Previously, you disabled the SRC client and reenabled it to start synchronization. The disabling of the SRC client's COPS support was undesirable for the applications that required resynchronization in addition to maintaining the COPS support. If the state of the SRC software is not synchronized with the router, the SRC software may be required to initiate resynchronization from the router.

The proprietary PIB provides the Policy Manager and QoS Manager functionality shown in the following lists.

- Policy Manager
  - Committed access rate
  - Packet filtering
  - Policy routing

  - QoS classification and marking
  - Rate limiting
  - Traffic class
- QoS Manager
  - Queues
  - Schedulers
  - Traffic classes

The JunosE-IP-PIB file is updated with each JunosE release. Since the PIB is implemented by both Juniper Networks SRC and JunosE devices, distribution of the PIB file to customers is not necessary. Customers can access the proprietary PIB file, on approval from Juniper Networks, through Juniper support.

Retrieval of DSL Line Rate Information from Access Nodes Overview

You can retrieve updated DSL line rate information from the Access Node Control Protocol (ANCP) and report this information to the SRC software with corresponding COPS messages. ANCP is also known as Layer 2 Control (L2C). To enable the router that functions as the SRC client to obtain updated line rate parameters from ANCP and transmit them to the COPS server, use the **sscc update-policy-request enable** command in Global Configuration mode. You can configure this setting on a per-virtual-router basis.

In networks with digital subscriber line access multiplexers (DSLAMs), after a connection is established between an subscriber and a routing gateway, the access node or DSLAM obtains the line rate information of the subscriber using a synchronization process. The line rate parameters are transferred in the COPS interface request by using the ANCP topology discovery message to the router that functions as the network access server (NAS). Typically, a COPS interface request is sent from the access node to the SRC client whenever an interface becomes operational.

You can configure the SRC client to obtain the line rate details from the access node whenever any change in the values of the parameters occurs. The capability to receive line rate data, when it changes on the access node, is disabled by default on the SRC client.

The access node passes the DSL line rate parameters, whenever they change, to the SRC client. The SRC client appends updated parameters to the COPS messages that it sends to the COPS server or SRC server. A COPS server processes the following topology parameters that it receives from the SRC client in the updated COPS messages:

- JunosElpInterfaceMode
- JunosElpInterfaceUpstreamRate
- JunosElpInterfaceDownstreamRate
- JunosElpInterfaceMinimumDataRateUpstream
- JunosElpInterfaceMinimumDataRateDownstream

- JunosElpInterfaceAttainableDataRateUpstream
- JunosElpInterfaceAttainableDataRateDownstream
- JunosElpInterfaceMaximumDataRateUpstream
- JunosElpInterfaceMaximumDataRateDownstream
- JunosElpInterfaceMinimumLowPowerDataRateUpstream
- JunosElpInterfaceMinimumLowPowerDataRateDownstream
- JunosElpInterfaceMaximumInterleavingDelayUpstream
- JunosElpInterfaceActualInterleavingDelayUpstream
- JunosElpInterfaceMaximumInterleavingDelayDownstream
- JunosElpInterfaceActualInterleavingDelayDownstream
- JunosElpInterfaceDSLlinestate

A COPS server that runs an SRC software release earlier than Release 3.0.0 does not support and process the preceding topology parameters that are appended to the COPS messages. Such COPS servers analyze the information, other than the parameters that describe updated DSL line rate details, that they receive in the COPS messages for policy management. Therefore, the COPS-PR operation ensures backward compatibility of the SRC clients with the COPS servers running SRC software releases earlier than Release 3.0.0 by ignoring the received line rate details.

When you configure the **sscc update-policy-request enable** command, a warning message is displayed, prompting you to confirm whether you want to enable the router that functions as the SRC client to forcibly send line rate information parameters to the COPS server, which is running a release of SRC software earlier than Release 3.0.0 that is not compatible with the line rate message format.

Even if you confirm the prompt to enable the SRC client to forcibly send updated DSL line rate parameters to the COPS server, the COPS server that is running a release of SRC software earlier than Release 3.0.0 ignores the updated line rate details that it receives and processes only the other information in the COPS messages.

The Policy Information Base (PIB) is modified to extend the JunosElpInterfaceEntry object. ANCP now notifies the SRC software about any change in the ANCP parameters. If this change in rate is greater than 10 percent or a change in mode, SRC software reports this upgrade to the service activation engine (SAE) in SRC version 3.0.0 and later.

Related Documentation

- SRC Client Configuration Overview on page 55
- Monitoring SRC Client Connection Status on page 253
- sscc update-policy-request enable

CHAPTER 11

Application Terminate Reasons

AAA Terminate Reasons

Table 7 on page 61 lists the default AAA terminate mappings. The table indicates the supported AAA terminate and deny reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 7: Default AAA Mappings

AAA Shutdown or Deny Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny address allocation failure	17	user error
deny address assignment failure	17	user error
deny application error	17	user error
deny authentication denied	17	user error
deny authentication failure	17	user error
deny authorization failure	17	user error
deny incompatible request	17	user error
deny invalid tunnel configuration	17	user error
deny limit exceeded	17	user error
deny mixed user types	10	nas request

Table 7: Default AAA Mappings *(continued)*

AAA Shutdown or Deny Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny no access challenge support	17	user error
deny no address allocation resources	17	user error
deny no resources	10	nas request
deny redirected authentication failure	17	user error
deny server not available	17	user error
deny server request timeout	17	user error
deny terminating user	10	nas request
deny unknown subscriber	17	user error
deny user termination	17	user error
shutdown address lease expiration	10	nas request
shutdown administrative reset	6	admin reset

Related Documentation

- Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37
- Monitoring Application Terminate Reason Mappings on page 283

L2TP Terminate Reasons

Table 8 on page 62 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 8: Default L2TP Mappings

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session access interface down	8	port error
session admin close	6	admin reset
session admin drain	6	admin reset

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings *(continued)*

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

- Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37
- Configuring Custom Mappings for PPP Terminate Reasons
- Monitoring Application Terminate Reason Mappings on page 283

PPP Terminate Reasons

Table 9 on page 79 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 9: Default PPP Mappings

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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 9: Default PPP Mappings *(continued)*

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
no ncps available	10	nas request
no network interface	10	nas request
no upper interface	9	nas error
osi admin disable	10	nas request
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

Related Documentation

- Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37
- Configuring Custom Mappings for PPP Terminate Reasons
- L2TP Terminate Reasons on page 62
- Monitoring Application Terminate Reason Mappings on page 283

RADIUS Client Terminate Reasons

Table 10 on page 86 lists the default RADIUS client terminate mappings. The table indicates the supported RADIUS client terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 10: Default RADIUS Client Mappings

RADIUS Client Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
no-acct-server	10	nas request
system-reboot	10	nas request
virtual-router-deletion	10	nas request

Related Documentation

- Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37
- Monitoring Application Terminate Reason Mappings on page 283

PART 2

Configuration

CHAPTER 12

Configuring B-RAS Services

Remote Access Configuration Tasks

Before you begin to configure B-RAS, you need to collect the following information for the RADIUS authentication and accounting servers:

- IP addresses
- User Datagram Protocol (UDP) port numbers
- Secret keys

Each configuration task is presented in a separate section in this chapter. Most of the B-RAS configuration tasks are optional.

To configure B-RAS, perform the following tasks:

1. Configure a B-RAS license.
2. (Optional) Map a user domain name to a virtual router. By default, all requests go through a default router.
3. (Optional) Set up domain name and realm name usage.
4. (Optional) Specify a single name for users from a domain.
5. Configure an authentication server on the router.
6. (Optional) Configure UDP checksums.
7. (Optional) Configure an accounting server on the router.
8. (Optional) Configure Domain Name System (DNS) and Windows Internet Name Service (WINS) name server addresses.
9. (Optional) Configure a local address pool for remote clients.
10. (Optional) Configure one or more DHCP servers.
11. Create a PPP interface on which the router can dynamically create an IP interface.
12. (Optional) Configure AAA profiles.
13. (Optional) Use vendor-specific attributes (VSAs) for Dynamic Interfaces.

14. (Optional) Set idle or session timeout.
15. (Optional) Limit the number of active subscribers on a virtual router (VR) or port.
16. (Optional) Set up the router to notify RADIUS when a user fails AAA.
17. (Optional) Configure a RADIUS download server on the router.
18. (Optional) Configure the Session and Resource Control (SRC) client (formerly the SDX client).
19. (Optional) Set baselines for AAA statistics or RADIUS authentication and accounting statistics.

Related Documentation

- Remote Access Overview on page 3

CHAPTER 13

Enabling the B-RAS Application

Configuring a B-RAS License

From Global Configuration mode, configure a B-RAS license:

```
host1(config)#license b-ras k3n91s6gvtj
```

B-RAS licenses are available in various sizes to enable subscriber access for up to one of the following maximum number of simultaneous active IP, LAC, and bridged Ethernet interfaces:

- 4000
- 8000
- 16,000
- 32,000
- 48,000

NOTE: To use a B-RAS license for 16,000 or more interfaces, each of your SRP modules must have 1 gigabyte (GB) of memory.

Related Documentation

- license b-ras on page 163

CHAPTER 14

Configuration Tasks for AAA Accounting

Configuring AAA Duplicate Accounting

To configure and enable duplicate accounting on a virtual router, you use the **aaa accounting duplication** command with the virtual router name to which AAA information is sent to the accounting server on that virtual router. For example, to enable duplicate accounting for the default virtual router:

```
host1(config)#aaa accounting duplication xyzCompanyServer
```

Related Documentation

- aaa accounting duplication on page 137

Configuring AAA Broadcast Accounting

To configure and enable broadcast accounting on a virtual router:

1. Create the virtual router group and enter VR Group Configuration mode:

   ```
   host1(config)#aaa accounting vr-group groupXyzCompany
   host1(vr-group-config)#
   ```

2. Add up to four virtual routers to the group. The accounting information will be sent to all virtual routers in the group.

   ```
   host1(vr-group-config)#aaa virtual-router 1 vrXyz1
   host1(vr-group-config)#aaa virtual-router 2 vrXyz2
   host1(vr-group-config)#aaa virtual-router 3 vrXyz3
   host1(vr-group-config)#exit
   host1(config)#
   ```

3. Enable broadcast accounting. Enter the correct virtual router context, and specify the virtual router group whose virtual routers will receive the accounting information.

   ```
   host1(config)#virtual-router opVr100
   host1:opVr100(config)#aaa accounting broadcast groupXyzCompany
   ```

Related Documentation
- aaa accounting broadcast on page 138
- aaa accounting vr-group on page 140
- virtual-router on page 193

Overriding AAA Accounting NAS Information

AAA accounting packets normally include two RADIUS attributes—NAS-IP-Address [4] and NAS-Identifier [32]—of the virtual router that generates the accounting information. You can override the default configuration and specify that accounting packets from particular broadcast virtual routers instead include the NAS-IP-Address and NAS-Identifier attributes of the authenticating virtual router.

To override the normal AAA accounting NAS information, access the correct virtual router context, and use the **radius override nas-info** command. For example:

```
host1(config)#virtual-router vrXyz1
host1:vrXyz1(config)#radius override nas-info
host1:vrXyz1(config)#virtual-router vrXyz2
host1:vrXyz2(config)#radius override nas-info
host1:vrXyz3(config)#exit
host1(config)#
```

Related Documentation
- radius override nas-info on page 165
- virtual-router on page 193

Collecting Accounting Statistics

You can use the **aaa accounting statistics** command to specify how the AAA server collects statistics on the sessions it manages. Use the **volume-time** keyword to specify that AAA notifies applications to collect a full set of statistics from each of their connections. Use the **time** keyword to specify that only the uptime status is collected for each connection. Collecting only uptime information reduces the amount of data sent to AAA and is a more efficient use of system resources for customers that do not need a full set of statistics. The router collects a full set of statistics by default.

Related Documentation
- aaa accounting statistics on page 139

CHAPTER 15

Configuration Tasks for AAA Servers

Configuring RADIUS AAA Servers

The number of RADIUS servers you can configure depends on available memory. The router has an embedded RADIUS client for authentication and accounting.

NOTE: You can configure B-RAS with RADIUS accounting, but without RADIUS authentication. In this configuration, the username and password on the remote end are not authenticated and can be set to any value.

You must assign an IP address to a RADIUS authentication or accounting server to configure it.

If you do not configure a primary authentication or accounting server, all authentication and accounting requests will fail. You can configure other servers as backup in the event that the primary server cannot be reached. Configure each server individually.

To configure an authentication or accounting RADIUS server:

1. Specify the authentication or accounting server address.

   ```
   host1(config)#radius authentication server 10.10.10.1
   host1(config-radius)#
   or
   host1(config)#radius accounting server 10.10.10.6
   host1(config-radius)#
   ```

2. (Optional) Specify a UDP port for RADIUS authentication or accounting server requests.

   ```
   host1(config-radius)#udp-port 1645
   ```

3. Specify an authentication or accounting server secret.

   ```
   host1(config-radius)#key gismo
   ```

4. (Optional) Specify the number of retries the router makes to an authentication or accounting server before it attempts to contact another server.

```
host1(config-radius)#retransmit 2
```

5. (Optional) Specify the number of seconds between retries.

```
host1(config-radius)#timeout 5
```

6. (Optional) Specify the maximum number of outstanding requests.

```
host1(config-radius)#max-sessions 100
```

7. (Optional) Specify the amount of time to remove a server from the available list when a timeout occurs.

```
host1(config-radius)#deadtime 10
```

8. (Optional) In Global Configuration mode, specify whether the E Series router should move on to the next RADIUS server when the router receives an Access-Reject message for the user it is authenticating.

```
host1(config)#radius rollover-on-reject enable
```

9. (Optional) Enable duplicate address checking.

```
host1(config)aaa duplicate-address-check enable
```

10. (Optional) Specify that duplicate accounting records be sent to the accounting server for a virtual router.

```
host1(config)#aaa accounting duplication routerBoston
```

11. (Optional) Enter the correct virtual router context, and specify the virtual router group to which broadcast accounting records are sent.

```
host1(config)#virtual-router vrSouth25
host1:vrSouth25(config)#aaa accounting broadcast westVrGroup38
host1:vrSouth25(config)#exit
```

12. (Optional) Specify that immediate accounting updates be sent to the accounting server when a response is received to an Acct-Start message.

```
host1(config)#aaa accounting immediate-update
```

13. (Optional) Specify whether the router collects all statistics or only the uptime status.

```
host1(config)#aaa accounting time
```

14. (Optional) Specify that tunnel accounting be enabled or disabled.

```
host1(config)#radius tunnel-accounting enable
```

15. (Optional) Specify the default authentication and accounting methods for the subscribers.

```
host1(config)#aaa authentication ppp default radius none
```

16. (Optional) Disable UDP checksums on virtual routers you configure for B-RAS.

```
host1:(config)#virtual router boston
host1:boston(config)#radius udp-checksum disable
```

Related Documentation

- aaa accounting broadcast on page 138
- aaa accounting duplication on page 137

- aaa accounting immediate-update
- aaa authentication default on page 141
- aaa duplicate-address-check on page 143
- key
- max-sessions
- radius accounting server on page 166
- radius authentication server on page 167
- radius rollover-on-reject on page 168
- radius tunnel-accounting on page 169
- radius udp-checksum on page 170
- retransmit on page 177
- timeout on page 191
- udp-port on page 192
- virtual-router on page 193

Configuring DNS Primary and Secondary NMS

To configure the DNS primary and secondary name server addresses:

1. Specify the IP address of the DNS primary name server.

   host1(config)#aaa dns primary 10.10.10.5

   or, for IPv6,

   host1(config)#aaa ipv6-dns primary 2001:db8::8001

2. Specify the IP address of the DNS secondary name server.

   host1(config)#aaa dns secondary 10.10.10.6

   or, for IPv6,

   host1(config)#aaa ipv6-dns secondary 2001:db8::8002

NOTE: The router uses name server addresses exclusively for PPP clients and not for domain name server resolution.

Related Documentation

- aaa dns on page 135
- aaa ipv6-dns on page 136

Configuring WINS Primary and Secondary NMS

To configure the WINS primary and secondary name server addresses:

1. Specify the IP address of the WINS primary name server.

   host1(config)#aaa wins primary 192.168.10.05

2. Specify the IP address of the WINS secondary name server.

   host1(config)#aaa wins secondary 192.168.10.40

NOTE: The router uses name server addresses exclusively for PPP clients and not for domain name server resolution.

Related Documentation

- aaa wins

CHAPTER 16

Configuration Tasks for AAA Authentication and User Database

Creating the AAA Local Authentication Environment

To create your local authentication environment:

1. Create local user databases—Create the default database or a named database.
2. Add entries to local user databases—Add user entries to the database. A database can contain information for multiple users.
3. Assign a local user database to the virtual router—Specify the database that the virtual router will use to authenticate subscribers.
4. Enable local authentication on the virtual router—Specify the **local** method as an AAA authentication method used by the virtual router.

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Local User Databases on page 101
- Adding AAA User Entries to Default Local User Databases on page 100
- Configuring AAA User Entries in Local User Databases on page 101
- Assigning a Local User Database to a Virtual Router on page 102
- Enabling Local Authentication on the Virtual Router on page 103

Creating AAA Local User Databases

When a subscriber connects to an E Series router that is using local authentication, the local authentication server uses the entries in the local user database selected by the virtual router to authenticate the subscriber.

A local authentication server can have multiple local user databases, and each database can have entries for multiple subscribers. The default local user database, if it exists, is used for local authentication by default. The E Series router supports a maximum of 100 user entries. A maximum of 100 databases can be configured.

To create a local user database, use the **aaa local database** command and the name of the database; use the name **default** to create the default local user database:

```
host1(config)#aaa local database westLocal40
```

Related Documentation

- Adding AAA User Entries to Local User Databases on page 101
- Adding AAA User Entries to Default Local User Databases on page 100
- Configuring AAA User Entries in Local User Databases on page 101
- Assigning a Local User Database to a Virtual Router on page 102
- Enabling Local Authentication on the Virtual Router on page 103
- aaa local database

Adding AAA User Entries to Default Local User Databases

The **username** command is similar to the command used by some third-party vendors. The command can be used to add entries in the default local user database; it is not supported for named local user databases. The IP address, IP address pool, and operational virtual router parameters are not supported in the **username** command. However, after the user is added to the default local user database, you can use the **aaa local username** command with a database name **default** to enter Local User Configuration mode and add the additional parameters.

NOTE: If the default local user database does not exist, the **username** command creates this database and adds the user entry to the database.

To add a subscriber and password or secret to the default local user database, complete the following step:

```
host1(config)#username rockyB password rockyPassword
```

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Local User Databases on page 101
- Configuring AAA User Entries in Local User Databases on page 101

- Assigning a Local User Database to a Virtual Router on page 102
- Enabling Local Authentication on the Virtual Router on page 103
- username

Adding AAA User Entries to Local User Databases

The local authentication server uses the information in a local user database to authenticate a subscriber. A local user database can contain information for multiple users.

The E Series router provides two commands for adding entries to local user databases: the **username** command and the **aaa local username** command. You can specify the following parameters:

- Username—Name associated with the subscriber.
- Passwords and secrets—Single words that can be encrypted or unencrypted. Passwords use two-way encryption, and secrets use one-way encryption. Both passwords and secrets can be used with PAP authentication; however, only passwords can be used with CHAP authentication.
- IP address—The IP address to assign to the subscriber (**aaa local username** command only).
- IP address pool—The IP address pool used to assign the subscriber's IP address (**aaa local username** command only).
- Operational virtual router—The virtual router to which the subscriber is assigned. This parameter is applicable only if the subscriber is authenticated by the default virtual router (**aaa local username** command only).

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Default Local User Databases on page 100
- Configuring AAA User Entries in Local User Databases on page 101
- Assigning a Local User Database to a Virtual Router on page 102
- Enabling Local Authentication on the Virtual Router on page 103
- **aaa local username on page 147**
- username

Configuring AAA User Entries in Local User Databases

To enter Local User Configuration mode and add user entries to a local user database, use the following commands:

1. Specify the subscriber's username and the database you want to use. Use the database name **default** to specify the default local user database. This command also puts the router into Local User Configuration mode.

   ```
   host1(config)# aaa local username cksmith database westLocal40
   host1(config-local-user)#
   ```

   NOTE: You can use the **aaa local username** command to add or modify user entries to a default database that was created by the **username** command.

2. (Optional) Specify the type of encryption algorithm and the password or secret that the subscriber must use to connect to the router. A subscriber can be assigned either a password or a secret, but not both. For example:

   ```
   host1(config-local-user)#password 8 iTtakes2%
   ```

3. (Optional) Specify the IP address to assign to the subscriber.

   ```
   host1(config-local-user)#ip-address 192.168.101.19
   ```

4. (Optional) Specify the IP address pool used to assign the subscriber's IP address.

   ```
   host1(config-local-user)#ip-address-pool svPool2
   ```

5. (Optional) Assign the subscriber to an operational virtual router. This parameter is applicable only if the subscriber is authenticated in the default virtual router.

   ```
   host1(config-local-user)#operational-virtual-router boston2
   ```

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Local User Databases on page 101
- Adding AAA User Entries to Default Local User Databases on page 100
- Assigning a Local User Database to a Virtual Router on page 102
- Enabling Local Authentication on the Virtual Router on page 103
- **aaa local username on page 147**
- ip-address
- ip-address-pool
- operational-virtual-router
- password

Assigning a Local User Database to a Virtual Router

Use the procedure in this section to assign a local user database to a virtual router. The virtual router uses the database for local authentication when the subscriber connects to the E Series router. Use the following commands in Global Configuration mode:

NOTE: If you do not specify a local user database, the virtual router selects the default database by default. This applies to all virtual routers.

1. Specify the virtual router name.

   host1(config)# virtual-router cleveland

2. Specify the database to use for authentication on this virtual router.

   host1:cleveland(config)# aaa local select database westLocal40

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Local User Databases on page 101
- Adding AAA User Entries to Default Local User Databases on page 100
- Configuring AAA User Entries in Local User Databases on page 101
- Enabling Local Authentication on the Virtual Router on page 103
- **aaa local select database on page 146**
- **virtual-router on page 193**

Enabling Local Authentication on the Virtual Router

On the E Series router, RADIUS is the default AAA authentication method for PPP subscribers. Use the commands in this section to specify that the local authentication method is used.

To enable local authentication on the default router, use the following command:

host1(config)# aaa authentication ppp default local

To enable local authentication on a specific virtual router, first select the virtual router:

host1(config)# virtual-router cleveland
host1:cleveland(config)# aaa authentication ppp default local

Related Documentation

- Creating AAA Local User Databases on page 100
- Adding AAA User Entries to Local User Databases on page 101
- Adding AAA User Entries to Default Local User Databases on page 100
- Configuring AAA User Entries in Local User Databases on page 101
- Assigning a Local User Database to a Virtual Router on page 102
- **aaa authentication default on page 141**
- **virtual-router on page 193**

CHAPTER 17

Configuration Tasks for Local Address Pools

Configuring a Local Address Server

You can create, modify, and delete address pools. You can display address pool information or status with the **show ip local pool** command. The following are examples of tasks you can configure:

- Specify an addressing scheme.

  ```
  host1(config)#ip address-pool local
  ```

- Map an address pool name to a range of local addresses. You can also use this command to add additional ranges to a pool.

  ```
  host1(config)#ip local pool addrpool_10 192.168.56.10 192.168.56.15
  ```

- Map a primary local address pool name to a domain name.

  ```
  host1(config)#aaa domain-map westford.com
  host1(config-domain-map)#address-pool-name poolA
  ```

- (Optional) Map a backup address pool to a domain name, which is used for address allocation if the primary local address pool is fully allocated.

  ```
  host1(config)#aaa domain-map westford.com
  host1(config-domain-map)#backup-address-pool-name backup_poolB
  ```

- (Optional) Map the domain name to the IPv6 local address pool, which is used for prefix delegation. If the authentication server returns the prefix pool name in the Framed-Ipv6-Pool attribute of the RADIUS-Accept-Request message, this value overrides the IPv6 local pool configured using the **ipv6-prefix-pool-name** command.

  ```
  host1(config)#aaa domain-map westford.com
  host1(config-domain-map)#ipv6-prefix-pool-name local_addr_pool
  ```

- Delete an address pool.

  ```
  host1(config)#no ip local pool addrpool_10
  ```

NOTE: If a pool or range is deleted and addresses are outstanding, the AAA server logs out the clients using the addresses.

- Create a shared local address pool.

  host1(config)#ip local shared-pool Shared_LAS_Pool_A DHCP_Pool_1

- Delete a shared local address pool.

  host1(config)#no ip local shared-pool Shared_LAS_Pool_C

- Set SNMP variables by specifying an existing pool name and values.

  host1(config)#ip local pool addrpool_10 warning 90 80

Related Documentation

- aaa domain-map on page 142
- address-pool-name
- backup-address-pool-name
- ip address-pool
- ip local pool
- ip local shared-pool
- ipv6-prefix-pool-name on page 160

Configuring the DHCPv6 Local Address Pools

The IPv6 local address pool for DHCP is an object that contains information about prefix configuration parameters and guidelines that govern the assignment of these prefixes to requesting routers. If you configured an interface for prefix delegation, the prefix assigned to that interface takes precedence over the prefix or range of prefixes configured at the router level in an IPv6 local pool.

To configure an IPv6 local address pool to be used for DHCPv6 prefix delegation:

1. Enable the IPv6 local address pool for to assign prefixes to the requesting router.

   host1(config)#ipv6 address-pool local

2. Configure the name of the IPv6 local address pool from which the delegating router assigns prefixes to the DHCPv6 client or requesting router.

   host1(config)#ipv6 local pool dhcpv6pd_pool

   NOTE: You must enable the IPv6 local address pool feature to be able to configure IPv6 local address pools.

3. Specify the IPv6 prefix range from which prefixes can be delegated to the DHCPv6 client. You can specify the prefix range in one of the following ways:

- Configure the prefix range by specifying an IPv6 prefix and the length of the prefix to be delegated. This prefix length is also called the assigned prefix length.

  host1(config-v6-local)#prefix 2002:2002::/32 48

  In this case, the starting and ending prefixes of the range are implicitly specified. In this example, the start of the range is 2002:2002::/48 and the end of the range is 2002:2002:ffff::/48. All prefixes assigned from this range have 48 as the prefix length.

- Alternatively, configure the prefix range by specifying the starting and ending IPv6 prefixes of the range.

  host1(config-v6-local)#prefix 3003:3003::/56 3003:3003:0:1000::/56

  In this case, the starting and ending prefixes of the range are explicitly specified. In the preceding example, a prefix range is configured with 16 prefixes that can be allocated to clients. All prefixes assigned from this range have 56 as the prefix length. When you specify the prefix range in this way, you must ensure that the starting and ending prefixes are of the same length.

4. Specify the time period when the requesting router can use the prefix. You can configure a preferred lifetime or a valid lifetime for the requesting router to use when you configure the prefix range. If no lifetime is specified when you configure the prefix range, the default lifetime of 1 day is assigned.

   NOTE: **The preferred lifetime must be less than or equal to the valid lifetime.**

   - Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).

     host1(config-v6-local)#prefix 5005:5005::/32 48 preferred 1 2 3 4

     In this example, the preferred lifetime is set to 1 day, 2 hours, 3 minutes, and 4 seconds. Because the valid lifetime is not configured, the default value of 1 day is assigned.

   - Use the **infinite** keyword to specify a lifetime that does not expire.

     host1(config-v6-local)#prefix 5005:5005::/32 48 valid infinite

     In this example, the period for which the prefix remains valid indefinitely for the requesting router to use after it has been delegated by the DHCPv6 server. In this case, the preferred lifetime is set to 1 day by default.

5. Specify the IPv6 address of the DNS servers to be returned to the client. You can configure a primary and secondary DNS server. The DNS server addresses are returned to the client in DHCPv6 responses as part of the DNS Recursive Name Server option.

   host1(config-v6-local)#dns-server 3001::1 3001::2

   If the DNS server is not configured in the IPv6 local address pool, the DNS server configured on the DHCPv6 local server is used to delegate prefixes. However, if DNS

servers are configured both in the IPv6 local pool and on the DHCPv6 local server, the values configured in the IPv6 local pool take precedence.

6. Specify the name of a DNS domain in the IPv6 local pool to be returned to clients in the DHCPv6 responses as part of the Domain Search List option. The client uses this domain name for DNS resolution. You can specify a maximum of four DNS domains for an IPv6 local pool's search list.

   ```
   host1(config-v6-local)#dns-domain-search test1.com
   host1(config-v6-local)#dns-domain-search test2.com
   ```

   You can configure one domain name per line. Enter the command on separate lines to configure additional domain names.

7. Set certain prefixes to be excluded from being allocated to the requesting router. You can exclude those addresses that are assigned to local interfaces. You can exclude specific prefixes or a range of prefixes from delegation to clients.

   ```
   host1(config-v6-local)#exclude-prefix 5005:5005:2::/48 5005:5005:a::/48
   ```

   In this example, all prefixes between the starting prefix of the range, 5005:5005:2::/48, and the ending prefix of the range, 5005:5005:a::/48 are excluded from allocation to clients.

8. Map the domain name to the IPv6 local address pool, which is used for prefix delegation. If the authentication server returns the prefix pool name in the Framed-Ipv6-Pool attribute of the RADIUS-Accept-Request message, this value overrides the IPv6 local pool configured using the **ipv6-prefix-pool-name** command.

   ```
   host1(config)#aaa domain-map westford.com
   host1(config-domain-map)#ipv6-prefix-pool-name local_addr_pool
   ```

   For more information about mapping domain names to the IPv6 local address pool, see ipv6-prefix-pool-name.

Related Documentation

- aaa domain-map on page 142
- dns-domain-search on page 148
- dns-server on page 149
- exclude-prefix on page 150
- prefix on page 156
- ipv6 address-pool local on page 158
- ipv6 local pool on page 159
- ipv6-prefix-pool-name on page 160

Configuring IPv6 Neighbor Discovery Local Address Pools

The IPv6 local address pool for Neighbor Discovery router advertisements is an object that contains information about prefix configuration parameters and guidelines that govern the assignment of these prefixes to requesting PPPv6 subscribers. If you configured an interface for the Neighbor Discovery router advertisements prefix, the prefix assigned

to that interface takes precedence over the prefix or range of prefixes configured at the router level in an IPv6 local address pool.

To configure an IPv6 local address pool to be used for Neighbor Discovery router advertisements:

1. Enable the IPv6 local address pool for Neighbor Discovery router advertisements to assign prefixes to the requesting PPPv6 subscribers.

   host1(config)#ipv6 address-pool ndra

2. Configure the name of the IPv6 local address pool for Neighbor Discovery router advertisements from which the delegating router assigns prefixes to the Neighbor Discovery router advertisements client or requesting router.

   host1(config)#ipv6 local ndra-pool ndra-pool1

   NOTE: **You must enable the IPv6 local address for Neighbor Discovery router advertisements feature to be able to configure IPv6 local address pools.**

3. Specify the IPv6 Neighbor Discovery router advertisements prefix range from which prefixes can be allocated to the Neighbor Discovery router advertisements client.

   Configure the prefix range by specifying the starting and ending IPv6 prefixes of the range. The prefix length should be /64. Any attempt to configure a prefix length other than /64 will show an error message.

   host1(config-v6-NdRa)#ndraprefix 3003:3003::/64 3003:3003:0:1000::/64

4. Set certain prefixes for Neighbor Discovery router advertisements to be excluded from being allocated to the requesting PPPv6 subscribers. You can exclude addresses that are assigned to local interfaces. You can exclude specific prefixes or a range of prefixes from allocation to clients.

   host1(config-v6-NdRa)#exclude-ndraprefix 5005:5005:2::/64 5005:5005:a::/64

   In this example, all prefixes between the starting prefix of the range 5005:5005:2::/64, and the ending prefix of the range 5005:5005:a::/64, are excluded from allocation to clients.

5. Map the domain name to the IPv6 local address pool, which is used for Neighbor Discovery router advertisements. If the authentication server returns the prefix pool name in the Framed-Ipv6-Pool attribute of the RADIUS-Accept-Request message, this value overrides the IPv6 local pool configured using the **ipv6-ndra-pool-name** command.

   host1(config)#aaa domain-map westford.com
   host1(config-domain-map)#ipv6-ndra-pool-name local_addr_pool

   For more information about mapping domain names to the IPv6 local address pool, see ipv6-ndra-pool-name.

Related Documentation

- IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview on page 46

CHAPTER 18

Configuring Clients Logging In to Interfaces

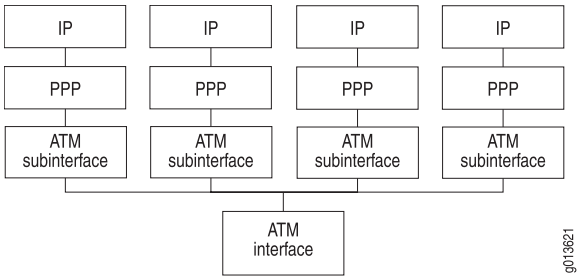
Creating an IP Interface

You can configure IP interfaces that support the following configurations:

Configuring Single PPP Clients per ATM Subinterface

Figure 3 on page 111 shows a conceptual view of the configuration of a single PPP client per ATM subinterface.

Figure 3: Single PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see *JunosE Link Layer Configuration Guide*.

1. Configure a physical interface.

   host1(config)#interface atm 0/1

2. Configure the subinterface.

   host1(config-if)#interface atm 0/1.20

3. Configure a permanent virtual circuit (PVC) by specifying the vcd (virtual circuit descriptor), the vci (virtual channel identifier), the vpi (virtual path identifier), and the encapsulation type.

   host1(config-if)#atm pvc 10 22 100 aal5snap

4. Configure PPP encapsulation.

   host1(config-if)#encapsulation ppp

5. Configure PAP or CHAP authentication.

   host1((config-if))#ppp authentication chap

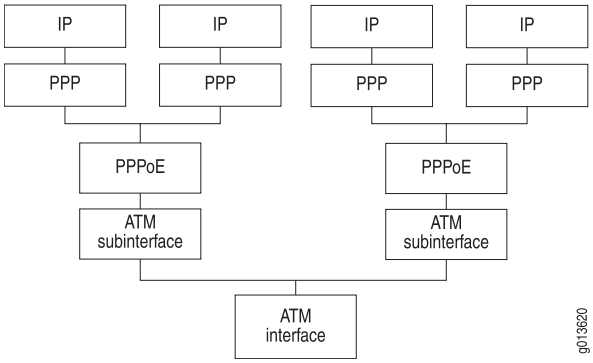
6. Assign a profile to the PPP interface.

   host1(config-subif)#profile foo

Configuring Multiple PPP Clients per ATM Subinterface

Figure 4 on page 112 shows how PPPoE supports multiplexing of multiple PPP sessions per ATM subinterface.

Figure 4: Multiple PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see *JunosE Link Layer Configuration Guide*.

1. Configure a physical interface.

   host1(config)#interface atm 0/1

2. Configure the subinterface.

   host1(config-if)#interface atm 0/1.20

3. Configure a PVC by specifying the vcd (virtual circuit descriptor), the vci (virtual channel identifier), the vpi (virtual path identifier), and the encapsulation type.

   host1(config-if)#atm pvc 10 22 100 aal5snap

4. Configure PPPoE encapsulation.

   host1(config-if)#encapsulation pppoe

5. Configure the subinterface for one PPP client.

```
host1(config-if)#interface atm 0/1.20.1
```

6. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

7. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

8. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

9. Configure the subinterface for a second PPP client.

```
host1(config-if)#interface atm 0/1.20.2
```

10. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

11. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

12. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

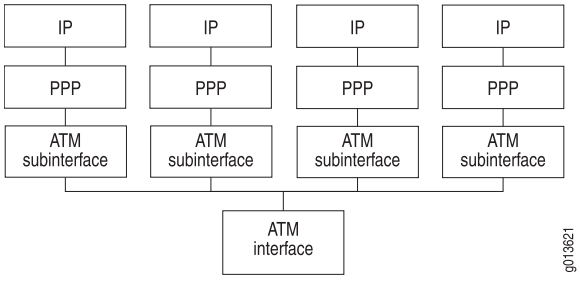
Related Documentation

- atm pvc
- encapsulation ppp
- interface
- ppp authentication
- profile

Configuring Single PPP Clients per ATM Subinterface

Figure 3 on page 111 shows a conceptual view of the configuration of a single PPP client per ATM subinterface.

Figure 5: Single PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see *JunosE Link Layer Configuration Guide*.

1. Configure a physical interface.

   host1(config)#interface atm 0/1

2. Configure the subinterface.

   host1(config-if)#interface atm 0/1.20

3. Configure a permanent virtual circuit (PVC) by specifying the vcd (virtual circuit descriptor), the vci (virtual channel identifier), the vpi (virtual path identifier), and the encapsulation type.

   host1(config-if)#atm pvc 10 22 100 aal5snap

4. Configure PPP encapsulation.

   host1(config-if)#encapsulation ppp

5. Configure PAP or CHAP authentication.

   host1((config-if))#ppp authentication chap

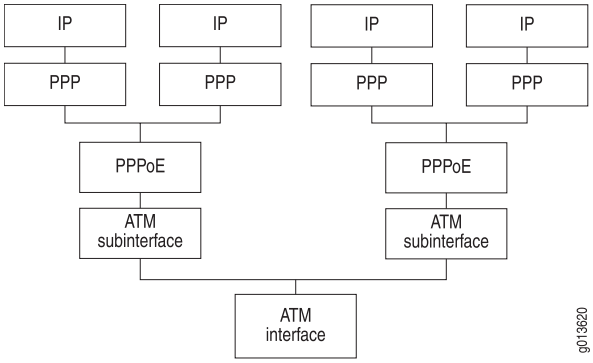
6. Assign a profile to the PPP interface.

   host1(config-subif)#profile foo

Configuring Multiple PPP Clients per ATM Subinterface

Figure 4 on page 112 shows how PPPoE supports multiplexing of multiple PPP sessions per ATM subinterface.

Figure 6: Multiple PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see *JunosE Link Layer Configuration Guide*.

1. Configure a physical interface.

   host1(config)#interface atm 0/1

2. Configure the subinterface.

   host1(config-if)#interface atm 0/1.20

3. Configure a PVC by specifying the vcd (virtual circuit descriptor), the vci (virtual channel identifier), the vpi (virtual path identifier), and the encapsulation type.

```
host1(config-if)#atm pvc 10 22 100 aal5snap
```

4. Configure PPPoE encapsulation.

```
host1(config-if)#encapsulation pppoe
```

5. Configure the subinterface for one PPP client.

```
host1(config-if)#interface atm 0/1.20.1
```

6. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

7. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

8. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

9. Configure the subinterface for a second PPP client.

```
host1(config-if)#interface atm 0/1.20.2
```

10. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

11. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

12. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

CHAPTER 19

Configuration Tasks for AAA Profiles

Controlling Access to Domain Names

You can control a PPP subscriber's access to certain domains on given interfaces. As the administrator, you can use the **deny** command to prevent PPP subscribers from using unauthorized domain names. Using the **allow** command, you can allow PPP subscribers to use authorized domain names.

In this example, the administrator wants to restrict access of a PPP interface to the specific domain **abc.com**.

1. Create an AAA profile.

   host1(config)#aaa profile restrictToABC

2. Specify the domain name you want to allow.

   host1(config-aaa-profile)#allow abc.com

3. Specify the domain name you want to restrict.

   host1(config-aaa-profile)#deny default

4. Associate the AAA profile to the designated PPP interface.

   host1(config-if)#ppp aaa-profile restrictToABC

When configured as such, the following is a likely scenario:

- PPP passes the AAA profile **restrictToABC** to AAA in the authentication request.
- AAA performs the following:

- Receives the authentication request from PPP with the subscriber's name **will@xyz.com**.
- Parses the domain name **xyz.com** and examines the specified AAA profile **restrictToABC**.
- Determines that the AAA profile **restrictToABC** is valid.
- Searches **restrictToABC** for a match on the PPP subscriber's domain name and finds no match.
- Searches **restrictToABC** for a match on the domain name **default**.
- Finds a match and denies the user access.

Related Documentation

- aaa profile
- allow
- deny
- ppp aaa-profile

Configuring an AAA Per-Profile Attribute List

JunosE Software enables you to configure AAA-specific attributes for subscribers attached to a specific PPP profile. If a per-profile list is configured, then only the attributes specified in the per-profile list are processed. If the per-profile list is not configured, then the existing standard attributes are configured.

NOTE: **The attributes supported by the per-profile list take precedence over the standard AAA attribute configuration. By default, the inclusion of all attributes is disabled in the per-profile list.**

This feature enables you to configure the following AAA attributes:

- **tunnel ignore nas-port**
- **tunnel ignore nas-port-type**

In this example, AAA-specific attributes are configured for subscribers attached to a specific PPP profile. You can configure this as follows:

1. Create an AAA per-profile attribute list, and configure the required AAA attributes in the list.

```
host1(config)#aaa per-profile-attr-list abc
host1 (config-perprofile-list)#action-type enable
host1 (config-perprofile-list)#attributes tunnel-ignore-nasport
  tunnel-ignore-nasport-type
```

2. Create an AAA profile.

```
host1(config)#aaa profile aaaprofile1
```

3. Specify the AAA attribute list in the AAA profile.

   host1(config-aaa-profile)#aaa-perprofilelist-name abc

4. Create a PPP profile.

   host1(config)#profile pppprofile1

5. Attach the AAA profile name to the PPP profile.

   host1(config-profile)#ppp aaa-profile aaaprofile1

6. To view the attributes configured in the AAA per-profile attribute list, issue the **show aaa per-profile-attr-list** command.

```
host1#show aaa per-profile-attr-list abc
Profile name: abc
Attribute Name              Status
---------------             --------
tunnel-ignore-nasport       enabled
tunnel-ignore-nasport-type  enabled
```

Related Documentation

- aaa profile
- aaa-perprofilelist-name
- aaa per-profile-attr-list (For Global Configuration)
- action-type
- attributes (AAA)
- ppp aaa-profile
- profile
- show aaa per-profile-attr-list

Configuring the NAS-Port-Type Attribute Manually

You can manually configure the NAS-Port-Type RADIUS attribute (attribute 61) in AAA profiles for ATM and Ethernet interfaces. Doing so allows AAA profiles to determine the NAS port type for a given connection.

To set the NAS-Port-Type attribute for ATM or Ethernet interfaces:

1. Create an AAA profile.

   host1(config)#aaa profile nasPortType

2. (Optional) Set the NAS-Port-Type attribute for ATM interfaces.

   host1(config-aaa-profile)#nas-port-type atm wireless-80211

3. (Optional) Set the NAS-Port-Type attribute for Ethernet interfaces.

   host1(config-aaa-profile)#nas-port-type ethernet wireless-cable

Related Documentation

- aaa profile

- nas-port-type atm
- nas-port-type ethernet

Configuring a Service Description for the AAA Profile

You can specify a service description that will be associated with an AAA profile. The description can then be exported through RADIUS by the Service-Description attribute (RADIUS attribute 26-53) in AAA profiles.

To set the Service-Description attribute:

1. Create the AAA profile.

   host1(config)#aaa profile xyzCorpPro2

2. Set the Service-Description attribute.

   host1(config-aaa-profile)#service-description bos-xyzcorp

Related Documentation

- aaa profile
- service-description

Configuring the Router to Obtain the LLID for a Subscriber

To configure the router to obtain the LLID for a subscriber:

1. Create an AAA profile that supports subscriber preauthentication.

   host1(config)#aaa profile preAuthLlid
   host1(config-aaa-profile)#pre-authenticate
   host1(config-aaa-profile)#exit

2. Define a RADIUS preauthentication server.

   host1(config)#radius pre-authentication server 10.10.10.1
   host1(config-radius)#key abc123
   host1(config-radius)#exit

3. Associate the AAA profile with the designated PPP interface.

   host1(config)#interface atm 4/3.101
   host1(config-subif)#ppp aaa-profile preAuthLlid

4. (Optional) Verify that preauthentication support is configured for the AAA profile.

```
host1(config-subif)#run show aaa profile name PreAuthLlid
preAuthLlid:
    atm nas-port-type: ADLSL-CAP
    ethernet nas-port-type: Cable
    profile-service-description: xyzService
    pre-authenticate
    allow xyz.com
    deny default
    translate xyz1.com abc.com
```

For information, see "Setting Baselines for Remote Access" on page 211.

5. (Optional) Verify configuration of the RADIUS preauthentication server.

```
host1(config-subif)#run show radius pre-authentication servers
                RADIUS Pre-Authentication Configuration
                ---------------------------------------
                 Udp     Retry              Maximum    Dead
 IP Address      Port    Count    Timeout   Sessions   Time   Secret
-------------   ----    -----    -------   --------   ----   ------
10.10.10.1      1812    3        3         255        0      radius
```

You can also display configuration information for preauthentication servers by using the **show radius servers** command. For information, see "Setting Baselines for Remote Access" on page 211.

6. (Optional) Display statistics for the RADIUS preauthentication server.

To display preauthentication statistics, use the **show radius pre-authentication statistics** command. For information, see "Setting Baselines for Remote Access" on page 211.

To display a count of preauthentication requests and responses, use the **show aaa statistics** command. For information, see "Setting Baselines for Remote Access" on page 211.

Related Documentation

- aaa profile
- interface
- key
- ppp aaa-profile
- pre-authenticate
- radius pre-authentication server
- show aaa profile on page 312
- show radius servers on page 336

CHAPTER 20

Configuration Task for Route-Download Servers for IPv4 and IPv6

Configuring the Route-Download Server to Download Routes

When you configure the E Series router as a route-download server, you specify the RADIUS server that you want to download the routes to your router. You can also modify the route-download server's default configuration parameters, such as when to start the download process each day, how often to downloaded routes, and how long to wait after a download error before retrying the process.

- To configure a RADIUS route-download server to download IPv4 routes:

  1. Specify the IP address and the key of the RADIUS server that you want to download routes.

     ```
     host1(config)#radius route-download server 192.168.1.17
     host1(config-radius)#key 35radsrv92
     ```

  2. (Optional) Specify the UDP port used for RADIUS route-download server requests.

     ```
     host1(config-radius)#udp-port 1812
     host1(config-radius)#exit
     host1(config)#
     ```

  3. Enable the route-download feature and optionally modify default parameters as needed.

     ```
     host1(config)#aaa route-download 1200 retry-interval 25 password Configured
       synchronization 03:45:00
     ```

  4. (Optional) Verify your route-download configuration:

     ```
     host1(config)#exit
     host1#show aaa route-download

     AAA Route Downloader:     configured in virtual router default
     Download Interval:        1200 minutes
     Retry Interval:           25 minutes
     Default Cost:             2
     Default Tag:              0
     Base User Name:           <HOSTNAME>
     ```

```
Password:                 Configured
Synchronization:          03:45:00

Status:                   downloading
Last Download Attempt:    TUE FEB 9 22:07:30 2007
Last Download Success:    <NEVER>
Last Regular Download:    not complete
Next Download Scheduled:  <DOWNLOAD ACTIVE>
Next Regular Download:    WED FEB 9 22:27:00 2007
```

- To configure a RADIUS route-download server to download IPv6 routes:

  1. Specify the IPv6 address and the key of the RADIUS server that you want to download routes.

     ```
     host1(config)#radius route-download server 192.168.1.17
     host1(config-radius)#key 35radsrv92
     ```

  2. (Optional) Specify the UDP port used for RADIUS route-download server requests.

     ```
     host1(config-radius)#udp-port 1812
     host1(config-radius)#exit
     host1(config)#exit
     ```

  3. Enable the route-download feature and optionally modify default parameters as needed.

     ```
     host1(config)#aaa route-download ipv6
     ```

  4. (Optional) Verify your route-download configuration:

     ```
     host1(config)#exit
     host1#show aaa route-download ipv6

     AAA Route Downloader:     configured in virtual router default
     Download Interval:        720 minutes
     Retry Interval:           10 minutes
     Default Cost:             2
     Default Tag:              0
     Base User Name:           <HOSTNAME>
     Password:                 <DEFAULT>
     Synchronization:          <NOT SET>

     Status:                   idle
     Last Download Attempt:    TUE DEC 13 2011 00:05:43 UTC
     Last Download Success:    TUE DEC 13 2011 00:05:43 UTC
     Last Regular Download:    complete
     Next Download Scheduled:  TUE DEC 13 2011 12:05:42 UTC
     Next Regular Download:    TUE DEC 13 2011 12:05:42 UTC
     ```

NOTE: If optional parameters such as retry-interval, synchronization, tag, cost, and download interval are configured for either IPv4 or IPv6 route downloads, they are applied to both IPv4 and IPv6 route downloads. However, the username and password are configured separately for IPv4 and IPv6 routes.

Related Documentation

- aaa route-download
- aaa route-download ipv6

- key
- radius route-download server
- show aaa route-download on page 313
- udp-port on page 192

CHAPTER 21

Configuration Tasks for Duplicate Prefixes Detection

Configuring Duplicate IPv6 Prefix Check

You can enable detection of duplicates of IPv6 Neighbor Discovery router advertisement prefixes and DHCPv6 delegated prefixes.

To enable detection of duplicate IPv6 prefixes:

From Global Configuration mode, enable the prefix-checking capability

```
host1(config)#aaa duplicate-prefix-check enable
```

Related Documentation

- Duplicate IPv6 Prefix Check Overview on page 51
- **aaa duplicate-prefix-check on page 144**

Configuring Detection of Duplicate IPv6 Prefixes in the AAA User Profile Database

You can enable detection of duplicates of IPv6 Neighbor Discovery router advertisement prefixes and DHCPv6 delegated prefixes in the AAA user profile database.

To enable enhanced detection of duplicate IPv6 prefixes:

- From Global Configuration mode, enable the enhanced duplicate IPv6 prefix-checking capability.

  ```
  host1(config)#aaa duplicate-prefix-check-extension enable
  ```

Related Documentation

- Duplicate IPv6 Prefix Detection in the AAA User Profile Database Overview on page 51
- Monitoring Duplicate IPv6 Prefixes in the AAA User Profile Database
- **aaa duplicate-prefix-check-extension on page 145**

CHAPTER 22

Configuring COPS Interworking with SRC Client

Configuring the SRC Client

You can configure SRC clients on a per-virtual-router basis. To configure the SRC client:

1. Enable the SRC client. With the CLI **sscc enable** command you can specify BER-encoded information exchange for COPS-PR.

   host1(config)#sscc enable cops-pr

2. Specify the IP addresses of up to three service activation engines (SAEs) (primary, secondary, and tertiary). You can optionally specify the port on which the SAEs listen for activity.

   host1(config)#sscc primary address
   host1(config)#sscc secondary address 192.168.12.1 port 3288

3. (Optional) Enable policy and QoS configuration support for IPv6 interfaces.

   host1(config)#sscc protocol ipv6

4. (Optional) Enable policy and QoS configuration support for L2TP interfaces on an L2TP access concentrator (LAC).

   host1(config)#sscc protocol lac

5. (Optional) Specify on which router the TCP/COPS connection is to be established.

   host1(config)#sscc transportRouter chicago

NOTE: If a COPS connection is in the open state (displayed in the "The Connection State is" field in the output of the **show sscc info** command), the router that you configure on which the COPS connection is to be established by using the **sscc transportRouter** *name* command does not take effect.

6. (Optional) Specify a fixed source address for the TCP/COPS connection created for an SRC client session.

   host1(config)#sscc sourceAddress 10.9.123.8

7. (Optional) Specify a fixed source interface for the TCP/COPS connection.

   host1(config)#sscc sourceInterface atm 3/0

8. (Optional) Specify the delay period during which the SRC client waits for a response from the SAE.

   host1(config)#sscc retryTimer 120

9. (Optional) Enable the user IP address mask to be sent to a Policy Decision Point (PDP) in place of the interface IP address mask for a virtual router.

   host1(config)#sscc option user-ip-mask-override

10. (Optional) Enable the calling station ID to be sent to a PDP for a virtual router.

    host1(config)#sscc option send-calling-station-id

    You can configure a virtual router to send the default calling station ID or the overridden calling station ID to the SRC Server irrespective of the RADIUS settings. If you want to enable the SRC client to send the Calling-Station-Id [31] RADIUS attribute to the COPS server only if this attribute is included in the RADIUS Access-Request, Acct-Start, or Acct- Stop messages, you can use the **radius-default-value** attribute with the **sscc option send-calling-station-id** command.

    host1(config)#sscc option send-calling-station-id radius-default-value

    If you want to enable the SRC client to send the Calling-Station-Id [31] RADIUS attribute to the COPS server, regardless of whether this attribute is included in the RADIUS Access-Request, Acct-Start, or Acct- Stop messages, you can use the **radius-overridden-value** attribute with the **sscc option send-calling-station-id** command.

    host1(config)#sscc option send-calling-station-id radius-overridden-value

    You must configure either the **radius calling-station-format** command or the **radius override calling-station-id remote-circuit-id** before you enable the functionality to cause the calling station ID to be always sent to the PDP for a virtual router, regardless of whether the ID is included or excluded from the Access-Request and Acct-Start messages.

NOTE: If you did not configure Calling-Station-Id attribute format using the **radius calling-station-format** command or did not configure the PPPoE remote circuit ID to be used in RADIUS messages instead of Calling-Station-Id using the **radius override calling-station-id** command, the Calling-Station-Id attribute is sent to the COPS server from the SRC client only if this attribute is contained in the RADIUS messages. In such a scenario, the attribute is not sent from the SRC client to the COPS server even if you configured the **sscc option send-calling-station-id radius-overridden-value** command.

11. (Optional) Enable the local QoS profile attachment information to be sent to a PDP for a virtual router.

    host1(config)#sscc option send-local-qos-profile-config

12. (Optional) Enable the LAC side NAS-IP address information to be sent to a PDP for a virtual router.

    host1(config)#sscc option send-lac-nas-ip

13. (Optional) Enable the LAC side NAS-Port information to be sent to a PDP for a virtual router.

    host1(config)#sscc option send-lac-nas-port

14. (Optional) Enable the SRC client to obtain updated line rate parameters from ANCP and transmit them to the COPS server.

    host1(config)#sscc update-policy-request enable

15. (Optional) Restart a COPS connection to, and resynchronize with, a PDP.

    host1#sscc restart

Related Documentation

- sscc address on page 187
- sscc enable on page 188
- sscc option on page 189
- sscc protocol ipv6
- sscc protocol lac
- sscc restart
- sscc retryTimer
- sscc sourceAddress
- sscc sourceInterface
- sscc transportRouter
- sscc update-policy-request enable

Configuring the Forwarding of COPS Requests to the SRC Server Based on DCM Profiles

You can configure the SRC client on an E Series router, which functions as the Common Open Policy Service (COPS) client, to send COPS messages to the SRC server or the COPS server based on the dynamic configuration manager (DCM) profile. For subscribers that use PPP links to establish sessions with the router or the SRC client and for which subscriber policies are managed by the SRC software, you can configure the setting in the PPP profiles to enable the SRC client to send COPS messages to the SRC server. This method of transmission of COPS request messages to the SRC server facilitates effective, optimal control of subscriber login events in the SRC software.

To configure a PPP profile with the setting to send COPS requests to the SRC server:

1. Create a PPP profile.

   host1(config)#profile pppprofile1

2. Configure the transmission of COPS request messages to the SRC server for all subscribers that are assigned this PPP profile.

   host1(config)#ip send-cops-request

   By default, COPS messages are sent to the SRC server. You must configure at least one IP configuration parameter in the PPP profile to enable the default behavior of the command to be effective. This functionality is applicable in environments where PPP links between the customer premises equipment (CPE) and the provider edge (PE) device or the router are configured for IPv4 or IPv6 subscriber sessions, either as independent or combined sessions. Also, this capability is effective only for dynamic PPP subscribers and not for DHCP and static subscriber sessions.

   Use the **no** version to disable the transmission of COPS messages from the SRC client to the SRC server for PPP subscribers.

Related Documentation

- ip send-cops-request on page 152

CHAPTER 23

Configuration Commands

aaa dhcpv6-ndra-pool override

Syntax [no] aaa dhcpv6-ndra-pool override

Release Information Command introduced in JunosE Release 13.0.0.

Description If the authentication server returns the Neighbor Discovery router advertisement prefix pool name in the RADIUS-Accept-Request message, it causes the Framed-Ipv6-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Delegated-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation. The **no** version of this command causes the Ipv6-NdRa-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Framed-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation. When the Ipv6-NdRa-Pool attribute is used for Neighbor Discovery, the prefix to be allocated to requesting routers or subscribers is obtained from the IPv6 local address pool for Neighbor Discovery. When the Delegated-Ipv6-Pool attribute is used for Prefix Delegation, the prefix to be delegated to the clients is obtained from the IPv6 local address pool for Prefix Delegation.

Mode Global Configuration

Related Documentation
- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108

aaa dns

Syntax aaa dns { primary | secondary } *ipAddress*

no aaa dns { primary | secondary }

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the IP address of the primary DNS name server. The **no** version sets the corresponding address to 0.

Options
- primary—Specifies the primary DNS name server
- secondary—Specifies the secondary DNS name server
- *ipAddress*—IP address of the name server

Mode Global Configuration

aaa ipv6-dns

Syntax aaa ipv6-dns { primary | secondary } *ipv6Address*

no aaa ipv6-dns { primary | secondary }

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the IPv6 address of the primary DNS name server. The **no** version sets the corresponding address to 0 (or ::).

Options
- primary—Specifies the primary DNS name server
- secondary—Specifies the secondary DNS name server
- *ipv6Address*—IPv6 address of the name server

Mode Global Configuration

aaa accounting duplication

Syntax aaa accounting duplication *routerName*

no aaa accounting duplication

Release Information Command introduced before JunosE Release 7.1.0.

Description Sends duplicate accounting records to the accounting server of a different virtual router. The **no** version disables the feature.

Options
- *routerName*—Virtual router name

Mode Global Configuration

aaa accounting broadcast

Syntax aaa accounting broadcast *vrGroupName*

no aaa accounting broadcast

Release Information Command introduced before JunosE Release 7.1.0.

Description Broadcasts accounting records for a virtual router to accounting servers of the virtual routers in the specified virtual router group. The **no** version disables the feature.

Options
- *vrGroupName*—Name of the virtual router group; a string of up to 32 characters

Mode Global Configuration

aaa accounting statistics

Syntax aaa accounting statistics { volume-time | time }

no aaa accounting statistics

Release Information Command introduced in JunosE Release 7.2.0.

Description Configures the router to collect either a full set of statistics or only uptime status for the sessions AAA is managing. Collecting only the uptime status is a more efficient use of system resources. The **no** version restores the default setting in which the router collects full statistics.

Options

- volume-time—Collects a full complement of statistics from each connection; the default setting
- time—Collects only uptime status for each connection

Mode Global Configuration

aaa accounting vr-group

Syntax [no] aaa accounting vr-group *vrGroupName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates an accounting virtual router group and enters VR Group Configuration mode. A virtual router group can have up to four virtual routers, whose accounting servers can receive broadcast accounting records. A group must contain at least one virtual router. The **no** version deletes the accounting virtual router group.

Options
- *vrGroupName*—Name of the virtual router group; a string of up to 32 characters

Mode Global Configuration

aaa authentication default

Syntax aaa authentication *subscriberType* default *authenticator* [*authenticator*]*

no aaa authentication *subscriberType* default

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the authentication method used for a particular type of subscriber. The **no** version produces the same result as specifying the **radius** value.

Options

- *subscriberType*—Type of subscriber:
  - atm1483—Specifies ATM 1483 subscribers
  - ip—Specifies IP subscriber management interfaces
  - ipsec—Specifies IPsec subscribers
  - ppp—Specifies PPP subscribers
  - radius-relay—Specifies RADIUS relay server subscribers
  - tunnel—Specifies tunnel subscribers
- *authenticator*—Authentication method:
  - none—Disables authentication, allowing all users access
  - local—Enables local authentication; supported for PPP subscribers only
  - radius—Enables RADIUS for authentication
  - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa domain-map

Syntax aaa domain-map *domainName*
[*routerName* [loopback *interfaceNumber* | *ipAddress ipMask*]]

no aaa domain-map *domainName*

Release Information Command introduced before JunosE Release 7.1.0.
ipAddress and *ipMask* variables added in JunosE Release 9.0.0.

Description Maps a user domain name to a virtual router. When you specify only the domain name, the command sets the mode to Domain Map Configuration. The **no** version deletes the map entry.

Options
- *domainName*—User domain name; specify the domain name *none* to assign users without domains to a specific virtual router.
- *routerName*—Router name associated with the domain name
- loopback—Specifies the loopback interface
- *interfaceNumber*—Interface number in the range 0–32000
- *ipAddress*—IP address of the local interface
- *ipMask*—IPv4 address mask of the local interface

Mode Global Configuration

aaa duplicate-address-check

Syntax aaa duplicate-address-check { enable | disable }

Release Information Command introduced before JunosE Release 7.1.0.

Description Allows you to enable or disable routing table address lookup or duplicate address check. There is no **no** version.

NOTE: To use this command, you must have a B-RAS license. Run the license b-ras command and enter your password.

Options
- enable—Specifies the feature; this is the default
- disable—Disables the feature

Mode Global Configuration

aaa duplicate-prefix-check

Syntax [no | default] aaa duplicate-prefix-check { enable | disable }

Release Information Command introduced in JunosE Release 11.2.0.

Description Configures AAA to enable duplicate IPv6 prefix-check in a virtual router context. Duplicate IPv6 prefix checking by AAA is disabled by default . The **default** version restores the default condition. The **no** version disables the duplicate IPv6 prefix-check capability.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default

Mode Global Configuration

aaa duplicate-prefix-check-extension

Syntax [no | default] aaa duplicate-prefix-check-extension { enable | disable }

Release Information Command introduced in JunosE Release 12.2.0.

Description Configures AAA to enable the enhanced duplicate IPv6 prefix-check in a virtual router context. Enhanced duplicate IPv6 prefix checking by AAA is disabled by default . The **no** version disables the enhanced duplicate IPv6 prefix-check capability.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default

Mode Global Configuration

aaa local select database

Syntax aaa local select database *databaseName*

no aaa local select

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns the local user database that the virtual router uses for local authentication. The **no** version restores the default setting, which uses the default local user database for local authentication.

Options
- *databaseName*—Name of the local user database

Mode Global Configuration

aaa local username

Syntax [no] aaa local username *userName* database *databaseName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a user entry in the specified local user database and enters Local User Configuration mode. The **no** version deletes the user entry from the specified local user database.

Options

- *userName*—User name of the subscriber
- *databaseName*—Name of the local user database; database name **default** configures the username in the default local user database

Mode Global Configuration

dns-domain-search

Syntax [no] dns-domain-search *domainName*

Release Information Command introduced in JunosE Release 10.1.0.

Description Specifies a list of domain names in the IPv6 local address pool to be returned to clients in DHCPv6 responses as part of the Domain Search List option. The **no** version removes the configured domain name.

NOTE: You can configure one domain name per line. Enter the command on separate lines to configure additional domain names.

Options

- *domainName*—Domain name that the DHCPv6 client uses when it resolves hostnames with the DNS server. You can specify a maximum of four DNS domains for the search list of an IPv6 local pool; maximum of 32 characters

Mode IPv6 Local Pool Configuration

dns-server

Syntax dns-server *ipAddressPrimary* [*ipAddressSecondary*]

no dns-server

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns a DNS server to an address pool. The **no** version removes the association between the address pool and the DNS server.

Options
- *ipAddressPrimary*—IP address of preferred DNS server
- *ipAddressSecondary*—IP address of secondary DNS server

Mode DHCP Local Pool Configuration

exclude-prefix

Syntax [no] exclude-prefix *Ipv6Prefix* [*endIpv6prefix*]

Release Information Command introduced in JunosE Release 10.1.0.

Description Specifies the IPv6 prefix or range of prefixes to exclude from being allocated to the requesting router. You can exclude those prefixes that have been assigned to local interfaces from being delegated to the DHCPv6 clients. The **no** version removes the IPv6 prefix or prefix range from the exclusion set and makes it available again for delegation to clients.

NOTE: If you attempt to exclude a prefix range that overlaps with another prefix range that has been already excluded from delegation to clients in the IPv6 local address pool, an error message is displayed and the configuration fails.

Options

- *Ipv6Prefix*—IPv6 prefix or the starting IPv6 prefix of the range of prefixes to be excluded from being delegated to the requesting router.
- *endIpv6Prefix*—Ending prefix of the range of IPv6 prefixes to be excluded from being delegated to the requesting router. If you specify this value, all prefixes from the starting IPv6 prefix up to this prefix are excluded from allocation.

Mode IPv6 Local Pool Configuration

exclude-ndraprefix

Syntax [no] exclude-ndraprefix *Ipv6Prefix* [*endIpv6prefix*]

Release Information Command introduced in JunosE Release 13.0.0.

Description Specifies the IPv6 prefix or range of prefixes to exclude from being allocated to the requesting router. You can exclude those prefixes that have been assigned to local interfaces from being delegated to the Neighbor Discovery router advertisement clients. The **no** version removes the IPv6 prefix or prefix range from the exclusion set and makes it available again for delegation to clients.

NOTE: If you attempt to exclude a prefix range that overlaps with another prefix range that has been already excluded from delegation to clients in the IPv6 local address pool, an error message is displayed and the configuration fails.

Options

- *Ipv6Prefix*—IPv6 prefix or the starting IPv6 prefix of the range of prefixes to be excluded from being delegated to the requesting router
- *endIpv6Prefix*—Ending prefix of the range of IPv6 prefixes to be excluded from being delegated to the requesting router. If you specify this value, all prefixes from the starting IPv6 prefix up to this prefix are excluded from allocation.

Mode IPv6 NdRa Pool Configuration

Related Documentation

- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108

ip send-cops-request

Syntax [no] ip send-cops-request

Release Information Command introduced in JunosE Release 13.3.0.

Description Enables the SRC client, which functions as the Common Open Policy Service (COPS) client, to send COPS messages to the SRC server or the COPS server based on the dynamic configuration manager (DCM) profile. This functionality is applicable only to dynamic PPP interfaces where the PPP links are configured for IPv4 or IPv6 subscriber sessions, either as independent or combined sessions. This behavior is not applicable for DHCP and static subscribers. By default, COPS messages are sent to the SRC server. You must configure at least one IP configuration parameter in the PPP profile to enable the default behavior of the command to be effective.

The **no** version disables the transmission of COPS messages from the SRC client to the SRC server for PPP subscribers.

Mode Profile Configuration

Related Documentation

- Configuring the Forwarding of COPS Requests to the SRC Server Based on DCM Profiles on page 131

ipv6 address

Syntax [no] ipv6 address *ipv6Prefix* [eui-64]

[no] ipv6 address [*ipv6Address maskLength* [eui-64]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns an IPv6 address (or network) to an interface and enables IPv6 processing on that interface. The **no** version deletes the association from the interface.

NOTE: The link-local address for an interface is automatically configured when IPv6 is enabled on the interface.

Options

- *ipv6Prefix*—Prefix that defines the IPv6 interface or network in the format *ipv6Address* **/** *length*, where
  - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d)
  - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
- *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d); the *ipv6Address* must appear in hexadecimal format using 16-bit values between colons. Refer to RFC 2373—IP Version 6 Addressing Architecture (July 1998) for details.
- *maskLength*—Length of the IPv6 mask. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
- eui-64—Specifies the use of the eui-64 interface identifier

Mode Interface Configuration, Profile Configuration

ipv6 nd

Syntax [no] ipv6 nd

Release Information Command introduced before JunosE Release 7.1.0.
Profile Configuration mode added in JunosE Release 9.0.0.

Description Enables the IPv6 Neighbor Discovery process on an interface. By default, the IPv6 Neighbor Discovery process is disabled on the router. However, if you configure an IPv6 address on a static interface, Neighbor Discovery process is automatically enabled. The **no** version disables the Neighbor Discovery process.

Mode Interface Configuration, Profile Configuration

ipv6 unnumbered

Syntax ipv6 unnumbered *interfaceType interfaceSpecifier*

no ipv6 unnumbered

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables IPv6 processing on an interface without assigning an explicit IPv6 address to that interface. The global IPv6 address of the interface, specified by the *interfaceType interfaceSpecifier* values, becomes the source address in packets that the unnumbered interface generates. Unnumbered interfaces are often used in point-to-point connections where an IPv6 address is not required. You must specify an interface location, which is the identifier of another interface on which the router has an assigned IPv6 address. This interface cannot be another unnumbered interface. The **no** version of the command removes the IPv6 address from the interface.

NOTE: Enabling IPv6 on an interface automatically configures the link-local address on an unnumbered interface.

Options

- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers

Mode Interface Configuration, Profile Configuration

prefix

Syntax prefix *startIpv6Prefix* { *assignedPrefixLength* | *endIpv6Prefix* } [[preferred | valid] { *days* [*hours* [*minutes* [*seconds*]]] | infinite }]

no prefix *startIpv6Prefix* [force | preferred [valid] | valid]

Release Information Command introduced in JunosE Release 10.1.0.

Description Specifies the prefix range from which IPv6 prefixes can be assigned to the DHCPv6 client. Also, configures the duration of time for which the requesting router can use the delegated prefix. If no value is specified for preferred or valid lifetime, the default lifetime of 1 day is used for the delegated prefix. The **no** version removes the IPv6 prefix range from the local address pool. You can also forcibly delete an IPv6 prefix range from which prefixes have been allocated.

NOTE: If you attempt to configure a prefix range that overlaps with an existing prefix range in the same pool, an error message is displayed and the configuration fails. Also, an error message is displayed if you try to configure a prefix range that overlaps with a prefix range in another IPv6 local address pool on the same virtual router.

Options

- *startIpv6Prefix*—Starting IPv6 prefix of the range of prefixes to be delegated to requesting routers.
- *endIpv6Prefix*—Ending IPv6 prefix of the range of prefixes to be delegated to requesting routers.
- *assignedPrefixLength*—Length of the IPv6 prefix to be assigned from this range of prefixes to the requesting router.
- preferred—Specifies use of the preferred period of time for the requesting router to use the prefix delegated by the DHCPv6 server. If the preferred lifetime is not specified, the prefix can be used by the requesting router for the default period of 1 day.
- valid—Specifies use of the valid period of time for the requesting router to use the prefix delegated by the DHCPv6 server. If the valid lifetime is not specified, the prefix can be used by the requesting router for the default period of 1 day.

NOTE: Although you can configure the valid lifetime for a prefix, the DHCPv6 server does not consider this value. The DHCPv6 server uses only the preferred lifetime for a prefix to determine the amount of time for which a prefix can be used by the requesting router.

- *days*—Number of days for the preferred or valid lifetime; in the range 0-32768.
- *hours*—Number of hours for the preferred or valid lifetime; in the range 0-24.

- *minutes*—Number of minutes for the preferred or valid lifetime; in the range 0-60.
- *seconds*—Number of seconds for the preferred or valid lifetime; in the range 0-60.
- infinite—Assigns a preferred or valid lifetime that does not expire for the delegated prefix.
- force—Forcibly deletes the IPv6 prefix range from the local address pool.

Mode IPv6 Local Pool Configuration

ipv6 address-pool local

Syntax [no] ipv6 address-pool local

Release Information Command introduced in JunosE Release 10.1.0.

Description Enables the IPv6 local address pool functionality to allow configuration of IPv6 local address pools to assign prefixes to DHCPv6 clients. The **no** version disables the IPv6 local address functionality.

NOTE: If you attempt to configure an IPv6 local address pool without enabling the IPv6 local pool feature, an error message is displayed.

Mode Global Configuration

ipv6 local pool

Syntax ipv6 local pool *poolName*

no ipv6 local pool *poolName* [force]

Release Information Command introduced in JunosE Release 10.1.0.

Description Accesses IPv6 Local Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use DHCPv6. The **no** version removes the IPv6 local pool.

Options

- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or DHCPv6 clients; string of up to 16 alphanumeric characters
- force—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to DHCPv6 clients is deleted, the corresponding DHCPv6 bindings are also deleted.

Mode Global Configuration

ipv6-prefix-pool-name

Syntax ipv6-prefix-pool-name *poolName*

no ipv6-prefix-pool-name

Release Information Command introduced in JunosE Release 10.1.0.

Description Specifies the IPv6 local prefix pool name to be used to delegate prefixes to the requesting router, when the RADIUS server does not return a pool name using the Framed-IPv6-Pool attribute. The **no** version removes the IPv6 local pool from the AAA domain map.

Options

- *poolName*—Name of the IPv6 local prefix pool to associate with the domain name; string of up to 16 alphanumeric characters

Mode Domain Map Configuration

ipv6 address-pool ndra

Syntax [no] ipv6 address-pool ndra

Release Information Command introduced in JunosE Release 13.0.0.

Description Enables the IPv6 local address pool functionality to allow configuration of IPv6 local address pools for Neighbor Discovery router advertisements to assign prefixes to Neighbor Discovery router advertisements. The **no** version disables the IPv6 local address functionality for Neighbor Discovery router advertisements.

NOTE: If you attempt to configure an IPv6 local address pools for Neighbor Discovery router advertisements without enabling the IPv6 local address pools for Neighbor Discovery router advertisements feature, an error message is displayed.

Mode Global Configuration

Related Documentation

- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108

ipv6 local ndra-pool

Syntax

ipv6 local ndra-pool *poolName*

no ipv6 local ndra-pool *poolName* [force]

Release Information

Command introduced in JunosE Release 13.0.0.

Description

Accesses IPv6 NdRa Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use Neighbor Discovery router advertisements. The **no** version removes the IPv6 local address pool.

Options

- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or Neighbor Discovery router advertisement clients; string of up to 16 alphanumeric characters
- force—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to Neighbor Discovery router advertisement clients is deleted, the corresponding Neighbor Discovery router advertisement bindings are also deleted.

Mode

Global Configuration

Related Documentation

- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108

license b-ras

Syntax license b-ras *licenseKey*

no license b-ras

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the B-RAS license provided by your sales representative or Juniper Networks Customer Service. Depending on the license purchased, the router supports up to 2,000, 4,000, 8,000, 16,000, or 20,000 authenticated PPP or SRC sessions. The **no** version disables the license.

Options

- *licenseKey*—Unique string of up to 15 alphanumeric characters that we provide to you

Mode Global Configuration

ndraprefix

Syntax ndraprefix *startIpv6Prefix* { *assignedPrefixLength* | *endIpv6Prefix* }

no ndraprefix *startIpv6Prefix* [force]

Release Information Command introduced in JunosE Release 13.0.0.

Description Specifies the prefix range from which IPv6 prefixes can be assigned to the Neighbor Discovery router advertisement client. The **no** version removes the IPv6 prefix range from the local address pool. You can also forcibly delete an IPv6 prefix range from which prefixes have been allocated.

NOTE: If you attempt to configure a prefix range that overlaps with an existing prefix range in the same pool, an error message is displayed and the configuration fails. Also, an error message is displayed if you try to configure a prefix range that overlaps with a prefix range in another IPv6 local address pool on the same virtual router. Also, an automatic truncation occurs if a higher prefix range is specified.

Options

- *startIpv6Prefix*—Starting IPv6 prefix of the range of prefixes to be delegated to requesting routers
- *endIpv6Prefix*—Ending IPv6 prefix of the range of prefixes to be delegated to requesting routers
- *assignedPrefixLength*—Length of the IPv6 prefix to be assigned from this range of prefixes to the requesting router
- force—Forcibly deletes the IPv6 prefix range from the local address pool

Mode IPv6 NdRa Pool Configuration

Related Documentation

- Configuring IPv6 Neighbor Discovery Local Address Pools on page 108

radius override nas-info

Syntax [no] radius override nas-info

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the RADIUS client for a virtual router context to override the standard use of the NAS-IP-Address [4] and NAS-Identifier [32] attributes when the client performs AAA broadcast accounting. Normally, AAA accounting packets include the NAS-IP-Address and NAS-Identifier attributes of the virtual router that generates the accounting information. However, this command specifies that the broadcast accounting packets instead include the authenticating virtual router's NAS-IP-Address and NAS-Identifier attributes. The **no** version restores the standard use of the two attributes in AAA accounting information.

Mode Global Configuration

radius accounting server

Syntax [no] radius accounting server *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the IP address of a RADIUS accounting server and puts the E Series router into RADIUS Configuration mode. The **no** version deletes the instance of the RADIUS server.

Options
- *ipAddress*—IP address of the server

Mode Global Configuration

radius authentication server

Syntax [no] radius authentication server *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the IP address of a RADIUS authentication server and puts the E Series router into RADIUS Configuration mode. The **no** version deletes the instance of the RADIUS server.

Options
- *ipAddress*—IP address of the server

Mode Global Configuration

radius rollover-on-reject

Syntax radius rollover-on-reject { enable | disable }

no radius rollover-on-reject

Release Information Command introduced before JunosE Release 7.1.0.

Description On a virtual router, specifies whether the router should roll over to the next RADIUS server when the router receives an access-reject message for the user it is authenticating. The **no** version restores the default value, disable.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius tunnel-accounting

Syntax radius tunnel-accounting { enable | disable }

no radius tunnel-accounting

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables tunnel accounting. The **no** version restores the default value, disable.

Options
- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius udp-checksum

Syntax radius udp-checksum { enable | disable }

no radius udp-checksum

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables UDP checksum for RADIUS packets on virtual routers that you configure for B-RAS. The **no** version restores the default value, enable.

Options
- enable—Specifies the feature; this is the default setting
- disable—Disables the feature

Mode Global Configuration

radius trap acct-server-responding

Syntax radius trap acct-server-responding { enable | disable }

no radius trap acct-server-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when a RADIUS accounting server returns to service after being marked as unavailable. The **no** version restores the default, disable.

Options
- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius trap acct-server-not-responding

Syntax radius trap acct-server-not-responding { enable | disable }

no radius trap acct-server-not-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when a RADIUS accounting server fails to respond to a RADIUS accounting request. The **no** version restores the default, disable.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius trap no-acct-server-responding

Syntax radius trap no-acct-server-responding { enable | disable }

no radius trap no-acct-server-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when all the configured RADIUS accounting servers per VR fail to respond to a RADIUS accounting request. The **no** version restores the default, disable.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius trap auth-server-responding

Syntax radius trap auth-server-responding { enable | disable }

no radius trap auth-server-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when a RADIUS authentication server returns to service after being marked as unavailable. The **no** version restores the default, disable.

Options
- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius trap auth-server-not-responding

Syntax radius trap auth-server-not-responding { enable | disable }

no radius trap auth-server-not-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when a RADIUS authentication server fails to respond to a RADIUS Access-Request message. The **no** version restores the default, disable.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

radius trap no-auth-server-responding

Syntax radius trap no-auth-server-responding { enable | disable }

no radius trap no-auth-server-responding

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables SNMP traps when all the configured RADIUS authentication servers per VR fail to respond to a RADIUS Access-Request message. The **no** version restores the default, disable.

Options

- enable—Specifies the feature
- disable—Disables the feature; this is the default setting

Mode Global Configuration

retransmit

Syntax retransmit *retries*

no retransmit

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the maximum number of times a router retransmits a RADIUS packet to an authentication or accounting server. The **no** version restores the default value.

Options
- *retries*—Number of retries, in the range 0–100; default value is 3

Mode RADIUS Configuration

snmp-server

Syntax [no] snmp-server

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the SNMP agent operation. The **no** version disables this operation.

Mode Global Configuration

snmp-server community

Syntax snmp-server community *commString* [view *viewName*] [*priv*] [*accessListName*]

no snmp-server community *commString*

Release Information Command introduced before JunosE Release 7.1.0.
view keyword and *viewName* variable added in JunosE Release 7.1.0.

Description Configures an authorized SNMP community and associates SNMPv1/v2c communities with SNMPv3 views. The **no** version removes an authorized community from the list of communities.

Options

- *commString*—Name of the SNMPv1/v2c community
- *viewName*—Name of the SNMPv3 view, which allows configuration using available dynamic views
- *priv*—Privileged Exec level: ro (read-only), rw (read-write), or admin (administrator)
- *accessListName*—Name of IP access list to filter SNMP clients

Mode Global Configuration

snmp-server enable traps

Syntax To enable and configure trap severity level on a global basis:

[no] snmp-server enable traps [*trapCategory* | snmp authentication]
[trapfilters *trapFilter*]

To specify the trap severity level on a per-category basis:

snmp-server enable traps { *trapCategory* | snmp authentication } per-category-trapFilters *trapFilter*

Release Information Command introduced before JunosE Release 7.1.0.
ip keyword added in JunosE Release 7.1.0.
packetMirror keyword added in JunosE Release 7.2.0.
per-category-trapFilters keyword added in JunosE Release 9.3.0.
ospfv3 trap category added in JunosE Release 13.2.0

Description Enables and configures global and category-level SNMP trap generation. The **no** version disables SNMP trap generation globally. There is no **no** version for the command to specify the trap severity level on a per-category basis.

Options

- *trapCategory*—SNMP trap category
  - addrPool—Local address pool traps
  - atmPing—E Series router proprietary ATM ping traps
  - bfdmib—BFD MIB traps
  - bgp—BGP state change traps
  - bulkstats—Bulkstats file full and nearly full traps
  - cliSecurityAlert—Security alerts traps
  - dhcp—DHCP traps
  - dismanEvent—Distributed management (disman) event traps
  - dosProtectionPlatform—DoS protection platform traps
  - dvmrp—DVMRP traps
  - dvmrpProp—E Series router proprietary DVMRP traps
  - environment—Power, temperature, fan, and memory utilization traps
  - fileXfer—File transfer status change traps
  - haRedundancy—High availability and redundancy traps
  - inventory—Router inventory and status traps
  - ip—Internet Protocol traps
  - ldp—LDP traps

  - link—SNMP linkUp and linkDown traps
  - log—System log capacity traps
  - mobileIpv4—Mobile IPv4 traps
  - mplste—Mplste traps
  - mrouter—Mrouter traps
  - ntp—E Series router proprietary traps
  - ospf—OSPF traps
  - ospfv3—OSPFv3 traps
  - packetMirror—Secure packet mirroring traps; visible only if packet mirroring is enabled
  - pim—PIM traps
  - ping—Ping operation traps (in disman remops MIB)
  - radius—RADIUS authentication and authorization servers
  - routeTable—Maximum route limit and warning threshold traps; when this trap is generated, the actual value of the exceeded warning threshold is displayed
  - sonet—SONET traps
  - snmp—SNMP coldStart, warmStart, link, and authenticationFailure traps
  - traceroute—Traceroute operation traps (in disman remops MIB)
  - vrrp—VRRP traps
- snmp—Specifies the SNMP coldStart, warmStart, and authenticationFailure traps
- authentication—Specifies the SNMP authenticationFailure trap
- *trapFilters*—Specifies the trap severity level at a global level; if the per-category trap severity level is not set for a particular category, this setting is applied to that category
- *trapFilter*—Minimum severity level for filtering traps at a global level or for a specified category
  - emergency—Severity level 0
  - alert—Severity level 1
  - critical—Severity level 2
  - error—Severity level 3
  - warning—Severity level 4
  - notice—Severity level 5
  - informational—Severity level 6
  - debug—Severity level 7

- per-category-trapFilters—Specifies the trap severity level for a particular category; this setting overrides the severity level set at the global level for this category
- *trapFilter*—Minimum severity level for filtering traps for the specified category

Mode Global Configuration

Related Documentation
- Monitoring SNMP Secure Packet Mirroring Traps

snmp-server host

Syntax To specify the SNMP version, community, UDP port, trap category and trap severity:

snmp-server host *ipAddress* [version *ver*] *securityString* [udp-port *port*]
[*trapCategory*]* [trapFilters *trapFilter*]

no snmp-server host *ipAddress*

To specify the ping timeout and trap queue:

snmp-server host *ipAddress* pingTimeOut *timeOutValue*
[trapQueue { drainRate *queueDrainRate* | full *queueFull* |
size *queueSize* }
[drainRate *queueDrainRate* | full *queueFull* | size *queueSize*]*]

snmp-server host *ipAddress* trapQueue
{ drainRate *queueDrainRate* | full *queueFull* | size *queueSize* }
[drainRate *queueDrainRate* | full *queueFull* | size *queueSize*]*
[pingTimeOut *timeOutValue*]

no snmp-server host *ipAddress* { pingTimeOut | trapQueue { drainRate | full | size } }

Release Information Command introduced before JunosE Release 7.1.0.
ip keyword added in JunosE Release 7.1.0.
packetMirror keyword added in JunosE Release 7.2.0.

Description Configures one or more hosts to receive an SNMP trap. The **no** version removes the specified host from the list of recipients.

Options

- *ipAddress*—IP address of the SNMP trap recipient
- *ver*—SNMP protocol version for traps sent to host; one of the following values: v1, v2c, or v3
- *securityString*—SNMP community string
- *port*—UDP port number of SNMP trap recipient
- *trapCategory*—SNMP trap category
  - addrPool—Local address pool traps
  - atmPing—E Series router proprietary ATM ping traps
  - bfdmib—BFD MIB traps
  - bgp—BGP state change traps
  - bulkstats—Bulkstats file full and nearly full traps
  - cliSecurityAlert—Security alerts traps
  - dosProtectionPlatform—DoS protection platform traps
  - dvmrp—DVMRP traps

  - dvmrpUni—E Series router proprietary DVMRP traps
  - environment—Power/temperature/fan traps
  - fileXfer—File transfer status change traps
  - inventory—Router inventory/status traps
  - ip—Internet Protocol traps
  - ldp—LDP traps
  - link—SNMP linkUp/linkDown traps
  - log—System log capacity traps
  - mobileIpv4—Mobile IPv4 traps
  - mplste—Mplste traps
  - mrouter—Mrouter traps
  - packetMirror—Secure packet mirroring traps; visible only if packet mirroring is enabled
  - ospf—OSPF traps
  - ping—Ping operation traps (in disman remops MIB)
  - radius—RADIUS traps
  - snmp—SNMP coldstart, warmstart, link, authenticationFailure traps
  - traceroute—Traceroute operation traps (in disman remops MIB)
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *trapFilter*—Minimum severity level for filtering traps sent to this host
  - alert—Severity level 1
  - critical—Severity level 2
  - debug—Severity level 7
  - emergency—Severity level 0
  - error—Severity level 3
  - informational—Severity level 6
  - notice—Severity level 5
  - warning—Severity level 4
- *timeOutValue*—Ping timeout in minutes, in the range 1–90; default value is 1
- trapQueue—Configures the SNMP trap queue for traps sent to this host
- *queueDrainRate*—Maximum number of traps per second to be sent to the host, in the range 0–2147483647; default value is 0. By default, there is no limit on the number of traps sent per second to the host.
- *queueFull*—Method used to drop traps when the trap queue is full

  - dropFirstIn—Drops the oldest trap in the queue
  - dropLastIn—Drops the most recent trap added to the queue
- *queueSize*—Maximum number of traps to be kept in the trap queue, in the range 32–214748364; default value is 32

Mode Global Configuration

Related Documentation
- Monitoring SNMP Secure Packet Mirroring Traps

snmp-server trap-source

Syntax snmp-server trap-source *interfaceType interfaceSpecifier*

no snmp-server trap-source

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the interface whose IP address is the source address for SNMP traps. The **no** version disables this feature.

Options

- *interfaceType*—Interface type; see Interface Types and Specifiers
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers

Mode Global Configuration

sscc address

Syntax sscc { primary | secondary | tertiary } address *ipAddress* [port *portNumber*]

no sscc { primary | secondary | tertiary } address [*ipAddress* [port *portNumber*]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the SRC client (formerly SSCC) with the IP addresses of the SRC servers and the ports on which the servers listen for activity. The **no** version removes the specified server (primary, secondary, or tertiary) from the list of SRC servers.

Options

- primary—Primary SRC server
- secondary—Secondary SRC server
- tertiary—Tertiary SRC server
- *ipAddress*—IP address of an SRC server
- *portNumber*—SRC server port number on which the server listens for activity; default port is 3288

Mode Global Configuration

sscc enable

Syntax sscc enable cops-pr

no sscc enable

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the SRC client's COPS support, which is used when the SRC service application engine communicates with a policy decision point, such as the SRC application. The **no** version disables COPS support.

Options
- cops-pr—Enables COPS-policy provisioning operation.

Mode Global Configuration

sscc option

Syntax sscc option { user-ip-mask-override | send-calling-station-id | radius-default-value | radius-overridden-value | send-local-qos-profile-config | send-lac-nas-ip | send-lac-nas-port }

no sscc option

Release Information Command introduced in JunosE Release 10.2.0.
send-calling-station-id keyword added in JunosE Release 11.1.0.
send-local-qos-profile-config keyword added in JunosE Release 11.2.0.
send-lac-nas-ip and **send-lac-nas-port** keyword added in JunosE Release 12.2.0.
radius-default-value and **radius-overridden-value** keywords added in JunosE Release 13.0.0.

Description When used with the **user-ip-mask-override** option, enables the user IP address mask to be sent to the Policy Decision Point (PDP) in place of the interface IP address mask for a virtual router. If user IP address mask is not available, then the interface IP address mask is sent. The **no** version disables user IP address mask override.

When used with the **send-calling-station-id** option, enables the calling station ID to be sent to the PDP for a virtual router. When used with the **radius-default-value** option, sends the default calling station ID to the PDP. When used with the **radius-overridden-value** option, sends the overridden calling station ID to the PDP. The **radius-overridden-value** option should be configured after configuring the **radius calling-station-format** command. If either the **radius calling-station-format** command or **radius override calling-station-id remote-circuit-id** command is not configured, then **radius-default-value** will be sent to the PDP instead of **radius-overridden-value**. The **no** version disables the option to send the calling station ID.

When used with the **send-local-qos-profile-config** option, enables the local QoS profile attachment information to be sent to the PDP for a virtual router. The **no** version disables the option to send the local QoS profile attachment information.

When used with the **send-lac-nas-ip** option, enables the LAC side NAS-IP address information to be sent to the PDP for a virtual router. The **no** version disables the option to send the NAS-IP address information.

When used with the **send-lac-nas-port** option, enables the LAC side NAS-Port information to be sent to the PDP for a virtual router. The **no** version disables the option to send the LAC side NAS-Port information.

Options

- user-ip-mask-override—Enables the user IP address mask to be sent to PDP
- send-calling-station-id—Enables the calling station ID to be sent to PDP
- radius-default-value—Enables the default calling station ID to be sent to the PDP
- radius-overridden-value—Enables the overridden calling station ID to be sent to the PDP

- send-local-qos-profile-config—Enables the local QoS profile attachment information to be sent to the PDP
- send-lac-nas-ip—Enables the LAC side NAS-IP address information to be sent to the PDP
- send-lac-nas-port—Enables the LAC side NAS-Port information to be sent to the PDP

Mode Global Configuration

timeout

Syntax RADIUS:

timeout *waitTime*

no timeout

RTR:

timeout *timeoutValue*

no timeout

Release Information Command introduced before JunosE Release 7.1.0.

Description When used from RADIUS Configuration mode, specifies the interval, in seconds, before the router retransmits a RADIUS packet to an authentication or accounting server. The **no** version restores the default.

When used from RTR Configuration mode, specifies the timeout for a Response Time Reporter operation. The **no** version returns the operation to the default value. You can apply this parameter only to *echo* entries.

Options

- *waitTime*—Number of seconds in the range 1–1000; default value is 3
- *timeoutValue*—Number in milliseconds that the operation waits for a response; if the value is set to 0 or is larger than frequency, it will be ignored; default value is 5000

Mode RADIUS Configuration, RTR Configuration

udp-port

Syntax udp-port *port*

no udp-port

Release Information Command introduced before JunosE Release 7.1.0.

Description From RADIUS Configuration mode, specifies the UDP port on the router where the RADIUS authentication, accounting, or dynamic-request servers reside. The router uses this port to communicate with the RADIUS servers. The **no** version restores the default value.

From RADIUS Relay Configuration mode, specifies the UDP port on the router where the RADIUS relay authentication or accounting server resides. The router uses this port to communicate with the RADIUS relay servers. The **no** version restores the default value.

Options

- *port*—Port number in the range 1–65535
  - 1812—Default for RADIUS and RADIUS relay authentication servers
  - 1813—Default for RADIUS and RADIUS relay accounting servers
  - 1700—Default for RADIUS dynamic-request servers

Mode RADIUS Configuration, RADIUS Relay Configuration

Related Documentation

- Configuring RADIUS-Based Packet Mirroring

virtual-router

Syntax virtual-router *vrName* | :*vrfName* | *vrName*:*vrfName*

no virtual-router *vrName* [wait-for-completion [*waitSeconds*]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates a virtual router or accesses the context of a previously created virtual router or a VRF. The **no** version deletes the virtual router, and the router defaults to the default virtual router. Issuing a **no** version that specifies an existing VRF only displays the error message: " Cannot delete a VRF with this command." You must use the **no ip vrf** command to remove a VRF.

NOTE: In Domain Map Configuration mode, the **virtual-router** command has been replaced by the router-name command and may be removed completely from Domain Map Configuration mode in a future release.

Options

- *vrName*—Name of the virtual router; a string of 1–32 alphanumeric characters
- :*vrfName*—Name of a VRF in the current VR context; a string of 1–32 alphanumeric characters
- *vrName*:*vrfName*—Name of a VRF in the context of a VR other than the current VR
- wait-for-completion—Specifies (in the absence of *waitSeconds*) that the CLI waits for completion of the **no** version operation before it returns a prompt, regardless of how long that takes
- *waitSeconds*—Number of seconds, in the range 1–64000, that the CLI waits before it returns a prompt, regardless of whether the **no** version operation has been completed

Mode Global Configuration, Privileged Exec

CHAPTER 24

Examples

Example: Domain Name and Realm Name

This section provides examples of possible domain or realm name results that you might obtain, depending on the commands and options you specify. This example uses the following username:

username: usEast/userjohn@abc.com@xyz.com

The router is configured with the following commands:

```
host1(config)#aaa delimiter domainName @!
host1(config)#aaa delimiter realmName /
```

Table 11 on page 195 shows the username and domain name that result from the parsing action of the various commands.

Table 11: Username and Domain Name Examples

Command	Resulting Username	Resulting Domain Name
aaa parse-order realm-first	userjohn@abc.com@xyz.com	usEast
aaa parse-order domain-first	userjohn@abc.com	xyz.com

Table 11: Username and Domain Name Examples *(continued)*

Command	Resulting Username	Resulting Domain Name
aaa parse-direction domainName right-to-left	userjohn@abc.com	xyz.com
aaa parse-direction domainName left-to-right	userjohn	abc.com@xyz.com
aaa parse-direction realmName right-to-left	userjohn@abc.com@xyz.com	usEast
aaa parse-direction realmName left-to-right	userjohn@abc.com@xyz.com	usEast

Related Documentation

- Domain Name and Realm Name Overview on page 9

Example: Stripping Domain Name Per Virtual Router for RADIUS Server Authentication

This example illustrates the final user name for a subscriber, based on the virtual router applied.

1. Configure the five virtual routers.

```
host(config)#profile VR1
host(config-profile)#ppp authentication virtual-router vr1 pap chap
host(config-profile)#exit
host(config)#profile VR2
host(config-profile)#ppp authentication virtual-router vr2 pap chap
host(config-profile)#exit
host(config)#profile VR3
host(config-profile)#ppp authentication virtual-router vr3 pap chap
host(config-profile)#exit
host(config)#profile VR4
host(config-profile)#ppp authentication virtual-router vr4 pap chap
host(config-profile)#exit
host(config)#profile VR5
host(config-profile)#ppp authentication virtual-router vr2 pap chap
host(config-profile)#exit
```

2. Access the context of a previously created virtual router and enable the strip domain functionality for each virtual router

```
host(config)#virtual-router vr1
host:vr1(config)#aaa strip-domain enable
host:vr1(config)#aaa strip-domain delimiter domainName $
host:vr1(config)#aaa strip-domain parse-direction domainName left-to-right
host:vr1(config)#radius authentication server 10.209.154.193
host:vr1(config)#key bras
host:vr1(config)#exit
host:vr1(config)#radius accounting server 10.209.154.193
host:vr1(config-radius)#key bras
```

```
host:vr1(config-radius)#exit
host:vr1(config)#virtual-router vr2

host:vr2(config)#aaa strip-domain enable
host:vr2(config)#aaa strip-domain parse-direction domainName left-to-right
host:vr2(config)#radius authentication server 10.209.154.194
host:vr2(config-radius)#key bras
host:vr2(config-radius)#exit
host:vr2(config)#radius accounting server 10.209.154.194
host:vr2(config-radius)#key bras
host:vr2(config-radius)#exit
host:vr2(config)#virtual-router vr3

host:vr3(config)#radius authentication server 10.209.154.193
host:vr3(config-radius)#key bras
host:vr3(config-radius)#exit
host:vr3(config)#radius accounting server 10.209.154.193
host:vr3(config-radius)#key bras
host:vr3(config-radius)#exit
host:vr3(config)#virtual-router vr4

host:vr4(config)#aaa strip-domain enable
host:vr4(config)#aaa strip-domain delimiter domainName %
host:vr4(config)#radius authentication server 10.209.154.194
host:vr4(config-radius)#key bras
host:vr4(config-radius)#exit
host:vr4(config)#radius accounting server 10.209.154.195
host:vr4(config-radius)#key bras
host:vr4(config-radius)#exit
host:vr4(config)#virtual-router vr5

host:vr5(config)#aaa strip-domain enable
host:vr5(config)#radius authentication server 10.209.154.193
host:vr5(config-radius)#key bras
host:vr5(config-radius)#exit
host:vr5(config)#radius accounting server 10.209.154.192
host:vr5(config-radius)#key bras
host:vr5(config-radius)#exit
```

Based on the virtual routers configuration, the Table 12 on page 197 below lists the final user name for each virtual router applied.

Table 12: aaa strip-domain Example

Subscribers	Virtual Router Applied	Final User Name
user1@123.com$test	VR1	user1@123.com
user2@123.com$test	VR2	user2
user3@123.com$test	VR3	user3@123.com$test
user4@123.com%test	VR4	user4@123.com

Table 12: aaa strip-domain Example *(continued)*

Subscribers	Virtual Router Applied	Final User Name
user5@123.com@test$test	VR5	user5@123.com

Related Documentation

- Overview of Mapping a User Domain to a Virtual Router on page 7
- Domain Name and Realm Name Overview on page 9

Example: Delegating the DHCPv6 Prefix

Consider a scenario in which a number of devices on a home network are connected to a customer premises equipment, CPE1, which is the requesting router. CPE1 is connected using a PPP link to the provider edge device, PE1, which is an E Series router operating as the DHCPv6 server or delegating router. After the IPv6 link is formed between CPE1 and PE1 and the IPv6 link-local address is created, CPE1 requests and obtains prefixes that are shorter than /64 (usually of length, /48) from PE1.

CPE1 is connected to the home network. CPE1 divides the single delegated prefix that it received from PE1 into multiple /64 prefixes and assigns one /64 prefix to each of the links in the home network. The address allocation mechanism in the subscriber network can be performed using ICMPv6 Neighbor Discovery in router advertisements, DHCPv6, or a combination of these two methods.

When PE1 receives a request for prefix delegation from CPE1, PE1 assigns prefixes from the list of unallocated prefixes in the IPv6 local pool.

The following sections of this example show how to delegate the DHCPv6 prefix:

- Order of Preference in Determining the Local Address Pool for Allocating Prefixes on page 198
- Order of Preference in Allocating Prefixes and Assigning DNS Addresses to Requesting Routers on page 199

Order of Preference in Determining the Local Address Pool for Allocating Prefixes

You can configure multiple local address pools on a virtual router. When multiple pools are configured, the pool that is used to allocate the prefix to the requesting router is selected using the following order of preference:

- If a pool name is returned by the RADIUS server in the Framed-IPv6-Pool attribute or in the Delegated-Ipv6-Pool attribute (VSA 26-161), that pool is used to delegate the prefix to the client.
- If the **aaa dhcpv6-ndra-pool override** command is not configured, and if the RADIUS server returns a pool name in the Framed-IPv6-Pool attribute, that pool name is used to delegate the prefix to the client.

- If the **aaa dhcpv6-ndra-pool override** command is configured, and if the RADIUS server returns a pool name in the Delegated-Ipv6-Pool attribute (VSA 26-161), that pool name is used to delegate the prefix to the client.
- If the RADIUS server does not return the pool name, the pool name configured in the AAA domain map (Ipv6-Prefix-Pool-Name) is used to delegate the prefix to the client.
- If no local address pool name is configured in the AAA domain map, the IPv6 address of the interface on which the request was received is used to determine the pool.
- If the interface address matches with any of the prefix ranges configured in the IPv6 local address pool on the router, that pool is used to delegate the prefix to the client.

Order of Preference in Allocating Prefixes and Assigning DNS Addresses to Requesting Routers

Prefix delegation can be configured at the interface level and at the router level. Also, certain VSA attributes returned in the RADIUS Access-Accept message from the authentication server can impact the selection of the prefix to be assigned to the requesting router. The level of preference attached to each of these prefix delegation configurations is crucial. The delegating router uses the following order of preference to determine the source from which the DHCPv6 prefix is delegated to the requesting router from the DHCPv6 server:

1. An interface that is configured for prefix delegation is given priority over the RADIUS attributes returned in the Access-Accept message or the prefixes configured in the IPv6 local address pool on the delegating router.
2. The RADIUS server might return one or more of the following attributes in the Access-Accept message in response to the client authentication request:
   - Ipv6-NdRa-Prefix (VSA 26-129)
   - Framed-IPv6-Prefix (RADIUS IETF attribute 97)
   - Delegated-IPv6-Prefix (RADIUS IETF attribute 123)
   - Framed-IPv6-Pool (RADIUS IETF attribute 100)
   - Delegated-Ipv6-Pool (VSA 26-161)

   If any of the first three attributes are returned, then the prefix contained in those attributes is used and the pool name in the Framed-IPv6-Pool/Delegated-Ipv6-Pool attribute is ignored. For example, if both the Delegated-IPv6-Prefix or Framed-IPv6-Prefix, and Framed-IPv6-Pool/Delegated-Ipv6-Pool attributes are returned from the RADIUS server, the DHCPv6 prefix delegation mechanism uses the Delegated-IPv6-Prefix attribute to advertise the prefix to clients.
3. If prefix delegation is not configured at the interface level and if no prefix is returned from the attribute in the RADIUS Access-Accept message, the prefix configured in the IPv6 local pool is delegated to the requesting router.

If you configured a list of IPv6 DNS servers and a string of domain names in the IPv6 local address pool, the order of preference in returning the DNS server address or domain name to the requesting client in the DHCPv6 response is as follows:

- Information returned from the RADIUS server for DNS servers only
- Information from the pool
- Locally configured DNS attributes

Related Documentation

- Example: Limiting the Number of Prefixes Used by DHCPv6 Clients on page 205
- DHCPv6 Local Address Pools for Allocation of IPv6 Prefixes Overview on page 44

Example: Configuring AAA Local Authentication

This example creates a sample local authentication environment. The steps in this example:

1. Create a named local user database (**westfordLocal40**).
2. Configure the database **westfordLocal40**.
   - Add users **btjones** and **maryrdavis** and their attributes to the database.
3. Create the default local database using the optional **username** command.
   - Add optional subscriber parameters for user **cksmith** to the default database.
4. Assign the default local user database to virtual router **cleveland**; assign database **westfordLocal40** to the default virtual router and to virtual router **chicago**.
5. Enable AAA authentication methods **local** and **none** on all virtual routers.
6. Use the **show** commands to display information for the local authentication environment (various **show** command displays are listed after the example).

Example 1

This example shows the commands you use to create the AAA local authentication environment.

```
host1(config)#aaa local database westfordLocal40
host1(config)#aaa local username btjones database westfordLocal40
host1(config-local-user)#secret 38schillCy
host1(config-local-user)#ip-address-pool addressPoolA
host1(config-local-user)#operational-virtual-router boston2
host1(config-local-user)#exit
host1(config)#aaa local username maryrdavis database westfordLocal40
host1(config-local-user)#secret 0 dav1sSecret99
host1(config-local-user)#ip-address 192.168.20.106
host1(config-local-user)#operational-virtual-router boston1
host1(config-local-user)#exit
host1(config)#username cksmith password 0 yourPassword1
host1(config)#aaa local username cksmith database default
host1(config-local-user)#ip-address-pool addressPoolA
host1(config-local-user)#operational-virtual-router boston2
host1(config-local-user)#exit
host1(config)#virtual-router cleveland
host1(config)#aaa local select database default
host1(config)#virtual-router default
host1(config)#aaa local select database westfordLocal40
```

```
host1(config)#virtual-router chicago
host1(config)#aaa local select database westfordLocal40
host1(config)#virtual-router default
host1(config)#aaa authentication ppp default local none
```

Example 2 This example verifies that local authentication is configured on the router.

```
host1#show aaa authentication ppp default
local none
```

Example 3 This example uses the **show configuration category aaa local-authentication** command with the **databases** keyword to show the local user databases that are configured on the router.

```
host1# show configuration category aaa local-authentication databases
! Configuration script being generated on TUE NOV 09 2004 12:50:18 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 8, 2004  18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication databases
!
hostname host1
aaa new-model
aaa local database default
aaa local database westfordLocal40
```

Example 4 This example uses the **local-authentication users** keywords to show the configured users and their parameters. The password for **username cksmith** is displayed unencrypted because the default setting of disabled or no for the **service password-encryption** command is used for the example. Secrets are always displayed encrypted.

```
host1# show configuration category aaa local-authentication users
! Configuration script being generated on THU NOV 11 2004 13:40:41 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 10, 2004  21:15)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication users
!
hostname host1
aaa new-model
aaa local username cksmith database default
 password yourPassword1
 operational-virtual-router boston2
 ip-address-pool addressPoolA
!
aaa local username btjones database westfordLocal40
 secret 5 }9s7-4N<WK2)2=)^!6~#
 operational-virtual-router boston2
 ip-address-pool addressPoolA
!
aaa local username maryrdavis database westfordLocal40
```



```
 secret 5 E@A:nDXJJ<irb\`mF#[j
 operational-virtual-router boston1
 ip-address 192.168.20.106
```

Example 5 This example uses the **users include-defaults** keywords to show the configured users and their parameters, including the default parameters **no-ip-address** and **no ip-address-pool**.

```
host1# show configuration category aaa local-authentication users include-defaults
! Configuration script being generated on TUE NOV 09 2004 13:09:03 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 8, 2004  18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication users
!
hostname host1
aaa new-model
aaa local username cksmith database default
 password yourPassword1
 operational-virtual-router boston2
 no ip-address
 ip-address-pool addressPoolA
!
aaa local username btjones database westfordLocal40
 secret 5 }9s7-4N<WK2)2=)^!6~#
 operational-virtual-router boston2
 no ip-address
 ip-address-pool addressPoolA
!
aaa local username maryrdavis database westfordLocal40
 secret 5 E@A:nDXJJ<irb\`mF#[j
 operational-virtual-router boston1
 ip-address 192.168.20.106
 no ip-address-pool
```

Example 6 This example uses the **virtual-router** keyword with the **default** specification to show the local user database that is used by the default virtual router.

```
host1# show configuration category aaa local-authentication virtual-router default
! Configuration script being generated on TUE NOV 09 2004 13:09:45 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 8, 2004  18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication
!
virtual-router default
aaa local select database westfordLocal40
```


Example 7 This example uses the **virtual-router** keyword with a named virtual router. The **include-defaults** keyword shows the default configuration, including the line showing that there is no named local user database selected.

```
host1# show configuration category aaa local-authentication virtual-router cleveland include-defaults
! Configuration script being generated on TUE NOV 09 2004 13:09:25 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 8, 2004  18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication
!
virtual-router cleveland
no aaa local select
```

Related Documentation

- aaa authentication default on page 141
- aaa local database
- aaa local select database on page 146
- aaa local username on page 147
- ip-address
- ip-address-pool
- operational-virtual-router
- password
- secret
- show aaa authentication default on page 302
- show configuration
- virtual-router on page 193

Example: Associating all Subscribers of a PPP Interface with a Specific Domain Name

In this example, an administrator wants to associate all subscribers of a PPP interface with a specific domain name.

1. Create an AAA profile.

   host1(config)#aaa profile forwardToXyz

2. Map the original domain name to the mapped domain name for domain map lookup.

   host1(config-aaa-profile)#translate default xyz.com

3. Associate the AAA profile with the designated PPP interface.

   host1(config-if)#ppp aaa-profile forwardToXyz

When configured as such, the following scenario is typical:

- PPP passes the AAA profile **forwardToXyz** to AAA in the authentication request.
- AAA performs the following tasks:
  - Receives the authentication request from PPP with the subscriber's name **morris@abc.com**.
  - Parses the domain name **abc.com** and examines the specified AAA profile **forwardToXyz**.
  - Determines that the AAA profile **forwardToXyz** is valid.
  - Searches **forwardToXyz** for a match on the PPP subscriber's domain name and finds no match.
  - Searches **forwardToXyz** for a match on the domain name **default**.
  - Finds a match and continues as normal using the domain name **xyz.com**.

NOTE: If there is no matching entry in the AAA profile for the user's domain name or for the domain name **default**, then AAA continues processing as if there were no AAA profile.

If the user's name does not contain a domain name, then AAA attempts to match to the domain name **none** in the AAA profile. If there is no entry for **none**, then AAA attempts to match for the domain name **default** in the AAA profile. If there is no entry for either **none** or **default**, then AAA continues processing as if there were no AAA profile.

Related Documentation

- aaa profile
- allow
- deny
- ppp aaa-profile
- translate

Example: Associating Multiple Domain Names with a Specific Domain Name

In this example, an administrator wants to use aliases; that is, to associate multiple domain names with a specific domain name and not allow other domain names.

1. Create an AAA profile.

   ```
   host1(config)#aaa profile toAbc
   ```

2. Map the original domain name to the mapped domain name for domain map lookup.

   ```
   host1(config-aaa-profile)#translate abc1.com abc.com
   host1(config-aaa-profile)#translate abc2.com abc.com
   host1(config-aaa-profile)#translate abc3.com abc.com
   ```

3. Specify the domain name you want to restrict.

```
host1(config-aaa-profile)#deny default
```

4. Associate the AAA profile with the designated PPP interface.

```
host1(config-if)#ppp aaa-profile toAbc
```

When configured as such, the following scenario is typical:

- PPP passes the AAA profile toAbc to AAA in the authentication request.
- AAA:
  - Receives the authentication request from PPP with the subscriber's name **jane@abc1.com**
  - Parses the domain name **abc1.com** and examines the specified AAA profile toAbc
  - Determines that the AAA profile **toAbc** is valid
  - Searches **toAbc** for a match on the PPP subscriber's domain name and finds a match
  - Continues as normal using the domain name **abc.com**

NOTE: If there is no matching entry in the AAA profile for the user's domain name or for the domain name **default**, then AAA continues processing as if there were no AAA profile.

If the user's name does not contain a domain name, then AAA attempts to match to the domain name **none** in the AAA profile. If there is no entry for **none**, then AAA attempts to match for the domain name **default** in the AAA profile. If there is no entry for either **none** or **default**, then AAA continues processing as if there were no AAA profile.

Related Documentation

- aaa profile
- allow
- deny
- ppp aaa-profile
- translate

Example: Limiting the Number of Prefixes Used by DHCPv6 Clients

If you a configure a very large prefix range in an IPv6 local address pool, the number of prefixes that can be used from that range by DHCPv6 clients is limited to 1048576.

Consider the following example in which an IPv6 local address pool, largePrefixRange, is configured. The prefix range is specified by the starting prefix and its length as 3003:3003::/32.

```
host1(config)#ipv6 local pool largePrefixRange
host1(config-v6-local)#prefix 3003:3003::/32 64
```

```
host1(config-v6-local)#end
```

The Total field of the output of the following **show ipv6 local pool largePrefixRange** and **show ipv6 local pool** commands indicates the number of prefixes that can be allocated to DHCPv6 clients: 1048756.

```
host1#show ipv6 local pool largePrefixRange

Pool : largePrefixRange
-----------------------
Utilization : 0
          Start                         End               Total    In Use
--------------------------   -------------------------   -------   -------
3003:3003::/64               3003:3003:ffff:ffff::/64    1048576   0
                                                Preferred      Valid
          Start              Exclude   Util    Lifetime     Lifetime
--------------------------   -------   ----   ----------   ----------
3003:3003::/64               0         0      1 day        1 day

host1#show ipv6 local pool
                         IPv6 Local Address Pools
                         ------------------------
      Pool                    Start                         End
----------------   -------------------------   -------------------------
largePrefixRange   3003:3003::/64              3003:3003:ffff:ffff::/64
      Pool          Total    In Use
----------------   -------   -------
largePrefixRange   1048576   0
```

Related Documentation

- show ipv6 local pool on page 330

Example: Using DHCPv6 Local Address Pools for Prefix Delegation over non-PPP Links

When a customer premises equipment (CPE) or requesting router and the provider edge (PE) router are connected using a PPP link, one of the following pool names is used to determine the IPV6 local address pool to be used for DHCPv6 Prefix Delegation to the CPE:

- The pool name returned by the RADIUS server in the Framed-IPv6-Pool attribute
- The pool name configured in the AAA domain map

However, for a CPE that is connected to the PE router using a non-PPP link, such as Ethernet, VLAN, or S-VLAN, the method for authentication of clients for DHCPv6 Prefix Delegation is not available in JunosE Release 10.1.x. In such cases, you can select the pool to be used for delegation of prefixes to the CPE by ensuring that the address of the interface over which the DHCPv6 request is received corresponds to any one of the prefix ranges in the configured local address pool.

The following example shows how you can configure an interface with an IPv6 address that matches a prefix configured in an IPv6 local address pool to enable allocation of prefixes from the configured pool for client requests over non-PPP links.

```
! Configure an IPv6 local address pool named example. Specify the IPv6 prefix
! range from which prefixes can be delegated to DHCPv6 clients by specifying an
! IPv6 prefix and the assigned prefix length. Configure the prefix 4004:4004::/48
! to be excluded from being allocated to the requesting client. Exit the IPv6 Local
! Pool Configuration mode.
host1(config)#ipv6 local pool example
host1(config-v6-local)#prefix 4004:4004::/32 48
host1(config-v6-local)#exclude-prefix 4004:4004::/48
host1(config-v6-local)#exit
!
! Create a loopback interface with the IPv6 address matching that of a prefix range
! configured in the example local pool. Exit the Interface Configuration mode.
host1(config)#interface loopback 1
host1(config-if)#ipv6 address 4004:4004::1/48
host1(config-if)#exit
!
! Create a Gigabit Ethernet interface and assign VLAN as the encapsulation
! method. Exit the Interface Configuration mode.
host1(config)#interface gigabitEthernet 2/1/4
host1(config-if)#encapsulation vlan
host1(config-if)#exit
!
! Create a VLAN subinterface, assign a loopback address to it, and enable
! IPv6 Neighbor Discovery. Exit the Interface Configuration mode.
host1(config)#interface gigabitEthernet 2/1/4.100
host1(config-if)#vlan id 100
host1(config-if)#ipv6 unnumbered loopback 1
host1(config-if)#ipv6 nd
host1(config-if)#exit
```

When the PE router receives a request for DHCPv6 Prefix Delegation over the gigabit Ethernet interface 2/1/4.100, prefixes are allocated to the client from the example local pool. In this example, the local pool to use for allocation of prefixes is selected based on the IPv6 address of the interface over which the request is received.

Related Documentation

- dns-domain-search on page 148
- dns-server on page 149
- exclude-prefix on page 150
- interface
- interface loopback
- ipv6 address on page 153
- ipv6 nd on page 154
- ipv6 unnumbered on page 155
- prefix on page 156
- ipv6 address-pool local on page 158
- ipv6 local pool on page 159
- ipv6-prefix-pool-name on page 160
- vlan id

PART 3

Administration

CHAPTER 25

Monitoring AAA Server and Authentication Settings

Setting Baselines for Remote Access

You can set baseline statistics using the **baseline** commands. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics.

Issue the **delta** keyword with the **show aaa statistics** command to show baselined statistics.

Setting a Baseline for AAA Statistics

Purpose Set a baseline for all AAA statistics.

Action Issue the **baseline aaa** command:

```
host1#baseline aaa
```

There is no **no** version.

Setting a Baseline for AAA Route Downloads

Purpose Set a baseline for route downloads.

Action
- Issue the **baseline aaa route-download** command for IPv4 routes:

  host1#baseline aaa route-download
- Issue the **baseline aaa route-download ipv6** command for IPv6 routes:

  host1#baseline aaa route-download ipv6

There is no **no** version.

Setting a Baseline for COPS Statistics

Purpose Set a baseline for COPS statistics.

Action Issue the **show cops statistics** command:

host1#show cops statistics

There is no **no** version.

Setting a Baseline for Local Address Pool Statistics

Purpose Set a baseline for local address pool statistics.

Action Issue the **show local pool statistics** command:

host1#show local pool statistics

There is no **no** version.

Setting a Baseline for RADIUS Statistics

Purpose Set a baseline for RADIUS statistics.

Action Issue the **show radius statistics** command:

host1#show radius statistics

There is no **no** version.

Setting the Baseline for SRC Statistics

Purpose Set a baseline for SRC statistics.

Action Issue the **show sscc statistics** command:

host#1show sscc statistics

There is no **no** version.

Related Documentation

- baseline aaa on page 294
- baseline aaa route-download on page 295
- baseline cops on page 296
- baseline local pool on page 297
- baseline radius on page 298
- baseline sscc on page 299

How to Monitor PPP Interfaces

Purpose Monitor PPP interfaces.

Action Use the following commands:

- **show ppp interface summary**
- **show ppp interface** *<selective control>*

For details on the **show ppp** commands, see *JunosE Link Layer Configuration Guide*.

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. For details, see *JunosE System Basics Configuration Guide*.

NOTE: AAA and RADIUS statistics are not preserved across a warm restart when stateful SRP Switchover is enabled.

Related Documentation

- Monitoring PPP Interfaces
- Monitoring Multilinked and Nonmultilinked PPP Interfaces

Monitoring the AAA Model

Purpose Display the AAA model.

Action To display the AAA model:

```
host1#show aaa model
aaa model: old model
```

Related Documentation

- show aaa model on page 310

Monitoring IP Addresses of Primary and Secondary DNS and WINS Name Servers

Purpose Display the IP addresses of the primary and secondary DNS and WINS name servers.

Action To display the IP addresses of the primary and secondary DNS and WINS name servers:

```
host1#show aaa name-servers
Name Server Addresses (for PPP Clients):
 primary DNS Addr                    10.2.3.4
 secondary DNS Addr                  10.6.7.8
 primary NBNS (WINS) Addr            10.22.33.44
 secondary NBNS (WINS) Addr          10.66.77.88
```

Meaning The IP addresses of DNS and WINS name servers are displayed.

Related Documentation

- show aaa name-servers on page 311

Monitoring AAA Server Attributes

Purpose Display status of the attributes on the AAA server, including AAA accounting duplication and broadcast.

For additional information about the **show configuration** command, see *JunosE System Basics Configuration Guide*.

Action To display status of the attributes on the AAA server, including AAA accounting duplication and broadcast:

```
host1#show configuration category aaa server-attributes include-defaults
! Configuration script being generated on FRI MAY 21 2010 07:52:13 UTC
! Juniper Edge Routing Switch ERX1440
! Version: 11.2.0 beta-1.1 [BuildId 12073] (April 22, 2010  11:46)
! Copyright (c) 1999-2010 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa server-attributes
!
virtual-router default
aaa accounting duplication lac
aaa accounting broadcast group1
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable
no aaa ipv6-nd-ra-prefix framed-ipv6-prefix
no aaa dhcpv6-delegated-prefix delegated-ipv6-prefix
aaa duplicate-prefix-check disable
!
! ================================================================================
!
```

```
virtual-router lac
no aaa accounting duplication
no aaa accounting broadcast
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable
no aaa ipv6-nd-ra-prefix framed-ipv6-prefix
no aaa dhcpv6-delegated-prefix delegated-ipv6-prefix
aaa duplicate-prefix-check disable
!
! ================================================================================
!
virtual-router isp
no aaa accounting duplication
no aaa accounting broadcast
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable
no aaa ipv6-nd-ra-prefix framed-ipv6-prefix
no aaa dhcpv6-delegated-prefix delegated-ipv6-prefix
aaa duplicate-prefix-check disable
```

Meaning Table 13 on page 215 lists the **show configuration category aaa server-attributes include-defaults** command output fields.

Table 13: show configuration category aaa server-attributes include-defaults Output Fields

Field Name	Field Description
virtual router	Name of the virtual router
aaa accounting duplication	Virtual router used for duplicate accounting
aaa accounting broadcast	Virtual router group used for broadcast accounting
aaa duplicate-address-check	Enabled, disabled
aaa accounting acct-stop on-aaa-failure	Enabled, disabled
aaa accounting acct-stop on-access-deny	Enabled, disabled
aaa subscriber limit per-vr	Enabled, disabled
aaa intf-desc-format include sub-intf	Enabled, disabled

Table 13: show configuration category aaa server-attributes include-defaults Output Fields *(continued)*

Field Name	Field Description
aaa intf-desc-format include adapter	Enabled, disabled
aaa accounting immediate-update	Enabled, disabled
aaa ipv6-nd-ra-prefix framed-ipv6-prefix	Framed-IPv6-Prefix RADIUS attribute used for IPv6 Neighbor Discovery router advertisements
aaa dhcpv6-delegated-prefix delegated-ipv6-prefix	Delegated-IPv6-Prefix RADIUS attribute used for DHCPv6 prefix delegation
aaa duplicate-prefix-check	Enabled, disabled

Related Documentation

- show configuration

Monitoring Configuration Information for AAA Local Authentication

Purpose

Display the configuration information for AAA local authentication. You can display information for the following keywords:

- - **databases**—Local user databases configured on the router
  - **users**—Users configured in the local user databases
  - **virtual-router**—Local user database selected by the specified virtual router for local authentication
- For additional information about the **show configuration** command, see *JunosE System Basics Configuration Guide*.

Action

To display the configuration information for AAA local authentication:

```
host1#show configuration category aaa local-authentication databases
! Configuration script being generated on TUE NOV 09 2004 12:50:18 UTC
! Juniper Edge Routing Switch ERX1400
! Version: 6.1.0 (November 8, 2004  18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication databases
!
hostname host1
aaa new-model
aaa local database default
aaa local database svaleLdb10
```

Meaning Table 14 on page 217 lists the **show configuration category aaa local-authentication** command output fields.

Table 14: show configuration category aaa local-authentication Output Fields

Field Name	Field Description
aaa local database	Name of the local user database; the name **default** specifies the default local user database
aaa local select database	Local user database that the virtual router uses for local authentication
aaa local username	Unique user entry in the local user database
database	Name of the local user database for the specified username
hostname	Name of the host router
ip-address	IP address parameter for the user entry
ip-address-pool	IP address pool parameter for the user entry
operational virtual-router	Virtual router parameter for the user entry
password	Password used to authenticate the subscriber
secret	Secret used to authenticate the subscriber
virtual-router	Name of virtual router

Related Documentation
- show configuration category aaa local-authentication

Monitoring the B-RAS License

Purpose Display the B-RAS license.

Action To display the B-RAS license:

```
host1#show license b-ras
K4bZ16Lr
```

Related Documentation
- show license on page 332 b-ras

CHAPTER 26

Monitoring AAA Accounting Details

Monitoring the AAA Accounting Configuration

Purpose Display the AAA accounting configuration.

Action To display the **show aaa accounting** command:

```
host1:vrXyz7#show aaa accounting

Accounting duplication set to router vrXyz25
Broadcast accounting uses group groupXyzCompany20
send acct-stop on AAA access deny is enabled
send acct-stop on authentication server access deny is disabled
acct-interval (for PPP Clients) 0
service-acct-interval 0
send immediate-update is enabled
```

Meaning Table 15 on page 219 lists the **show aaa accounting** command output fields.

Table 15: show aaa accounting Output Fields

Field Name	Field Description
Accounting duplication	Name of the virtual router to which duplicate accounting records are sent to the accounting server
Broadcast accounting	Name of the virtual router groups to which broadcast accounting records are sent to the accounting server
send acct-stop on AAA access deny	Enabled, disabled
send acct-stop on authentication server access deny	Enabled, disabled
acct-interval (for PPP Clients)	Number of minutes between accounting update operations

Table 15: show aaa accounting Output Fields *(continued)*

Field Name	Field Description
service-acct-interval	Number of minutes between interim accounting updates for services created by the Service Manager feature
send immediate-update	On receipt of response to Acct-Start message; enabled, disabled

Related Documentation

- show aaa accounting on page 300

Monitoring AAA Accounting Default

Purpose Display the AAA accounting default method for a subscriber type.

You can view the method used for ATM 1483, IPSec, PPP, RADIUS relay server, and tunnel subscribers, and IP subscriber management interfaces.

Action To display the default AAA accounting method:

```
host1#show aaa accounting tunnel default
radius
```

Related Documentation

- show aaa accounting default on page 301

Monitoring the AAA Accounting Interval

Purpose Display the accounting interval.

Action To display the accounting interval:

```
host1#show aaa accounting interval
acct-interval (for PPP Clients) 10
```

Related Documentation

- show aaa accounting interval

Monitoring AAA Specific Virtual Router Groups

Purpose Display the names of a specific virtual router group or of all virtual router groups configured on the router, and of the virtual routers making up the groups.

Action To display the names of a specific virtual router group or of all virtual router groups configured on the router. Display the virtual routers making up the groups:

```
host1#show aaa accounting vr-group
vr-group groupXyzCompany10:
 virtual-router 1 vrXyzA
 virtual-router 2 vrXyzB
```

```
 virtual-router 3 vrXyzC
 virtual-router 4 vrXyzD
vr-group groupXyzCompany20:
 virtual-router 1 vrXyzP
 virtual-router 2 vrXyzQ
 virtual-router 3 vrXyzR
 virtual-router 4 vrXyzS
```

Meaning Table 16 on page 221 lists the **show aaa accounting vr-group** command output fields.

Table 16: show aaa accounting vr-group Output Fields

Field Name	Field Description
vr-group	Name of the virtual router group

Related Documentation

- Configuring AAA Broadcast Accounting on page 93
- show aaa accounting vr-group

CHAPTER 27

Monitoring the Mapping of User Domains to Virtual Routers

Monitoring the Default AAA Authentication Method List

Purpose Display the default AAA authentication method list for a subscriber type. You can view the method list used for ATM 1483 subscribers, IPSec subscribers, IP subscriber management interfaces, PPP subscribers, RADIUS relay subscribers, and tunnel subscribers.

For example, you can verify that the local authentication method is configured for PPP subscribers.

Action To display the default AAA authentication method list for a subscriber type:

```
host1#show aaa authentication ppp default
local none
```

Related Documentation

- show aaa authentication default on page 302

Monitoring AAA Domain Name Stripping for a Domain Per Virtual Router

Purpose Display information about the aaa domain-name stripping functionality per virtual router.

Action To display information about the aaa domain-name stripping functionality per virtual router:

```
host1:vr1(config)#show aaa strip-domain
strip-domain is disable
strip-domain domainName delimiter is “@”
strip-domain domainName parse direction is right-to-left
```

Meaning Table 17 on page 224 lists the **show aaa strip-domain** command output fields.

Table 17: show aaa strip-domain Output Fields

Field Name	Field Description
delimiter	Delimiter value configured for the subscriber's domain
domainName	The domain name characteristics configured for the broadband remote access subscriber per virtual router
disable	The domain name stripping functionality is disabled for the virtual router
enable	The domain name stripping functionality is enabled for the virtual router
left-to-right	The parsing direction configured for stripping the domain name at the virtual router is left-to-right
right-to-left	The parsing direction configured for stripping the domain name at the virtual router is right-to-left

Related Documentation

- aaa domain-map on page 142
- ppp authentication
- show aaa delimiters on page 303
- show aaa strip-domain on page 304

Monitoring Mapping Between User Domains and Virtual Routers

Purpose Display the mapping between user domains and virtual routers.

The following keywords have significance when used as user domains:

- **none**—All client requests with no user domain name are associated with the virtual router mapped to the **none** entry
- **default**—All client requests with a domain present that have no map are associated with the virtual router mapped to the **default** entry

Action To display the mapping between user domains and virtual routers:

```
host1#show aaa domain-map
Domain: lac-tunnel; auth-router-name: lac;
ip-router-name: default; ipv6-router-name: default
Tunnel                Tunnel   Tunnel   Tunnel    Tunnel
 Tag     Tunnel Peer  Source    Type    Medium   Password    Tunnel Id
------   -----------  ------   ------   ------   --------   -----------
5        192.168.1.1  <null>   l2tp     ipv4     welcome    lac-tunnel

                      Tunnel                Tunnel
Tunnel     Tunnel     Server     Tunnel      Max
```

```
 Tag     Client Name    Name    Preference   Sessions     Tunnel RWS
------   -----------   ------   ----------   --------   --------------
5        lac           boston   5            0          4

                                                        Tunnel
         Tunnel     Tunnel            Tunnel       Tx
Tunnel   Virtual    Failover           Switch     Speed
 Tag     Router      Resync           Profile     Method
------   -------   --------         ---------    ------
5        <null>    silent failover   denver      qos
```

Meaning Table 18 on page 225 lists the **show aaa domain-map** command output fields.

Table 18: show aaa domain-map Output Fields

Field Name	Field Description
Domain	Name of the domain
auth-router-name	Access virtual router to which user domain name is mapped
ip-router-name	IPv4 virtual router to which user domain name is mapped
router-mask	IP mask of the local interface
tunnel-group	Name of the tunnel group assigned to the domain map
ipv6-router-name	IPv6 virtual router to which user domain name is mapped
local-interface	Interface information to use on the local (E Series) side of the subscriber's interface
ipv6-local-interface	IPv6 interface information to use on the local (E Series) side of the subscriber's interface
poolname	Local address pool from which the router allocates addresses for this domain
IP hint	IP hint is enabled
strip-domain	Strip domain is enabled
override-username	Single username used for all users from a domain in place of the values received from the remote client
override-password	Single password used for all users from a domain in place of the values received from the remote client
Tunnel Tag	Tag that identifies the tunnel
Tunnel Peer	Destination address of the tunnel

Table 18: show aaa domain-map Output Fields *(continued)*

Field Name	Field Description
Tunnel Source	Source address of the tunnel
Tunnel Type	L2TP
Tunnel Medium	Type of medium for the tunnel; only IPv4 is supported
Tunnel Password	Password for the tunnel
Tunnel Id	ID of the tunnel
Tunnel Client Name	Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
Tunnel Server Name	Host name expected from the peer (the LNS) when during tunnel startup
Tunnel Preference	Preference level for the tunnel
Tunnel Max Sessions	Maximum number of sessions allowed on a tunnel
Tunnel RWS	L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by system chooses
Tunnel Virtual Router	Name of the virtual router to map to the user domain name
Tunnel Failover Resync	L2TP peer resynchronization method
Tunnel Switch Profile	Name of the L2TP tunnel switch profile
Tunnel Tx Speed Method	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

Related Documentation

- show aaa domain-map on page 305

Monitoring Tunnel Subscriber Authentication

Purpose Verify configuration of tunnel subscriber authentication. When authentication is enabled, the output indicates this configuration. When authentication is disabled, the output presents no information about the configuration.

Action To display tunnel subscriber authentication configuration:

```
host1#show aaa domain-map
Domain: tunnel.com; auth-router-name: default; ip-router-name: default
ipv6-router-name: default; tunnel-subscriber authentication: enable
```

Meaning Authentication is enabled.

Related Documentation

- show aaa domain-map on page 305

CHAPTER 28

Verifying Settings for Detection of Duplicate Prefixes

Monitoring Routing Table Address Lookup

Purpose Display whether the routing table address lookup or duplicate address check is enabled or disabled.

Action To display whether the routing table address lookup or duplicate address check is enabled or disabled:

```
host1#show aaa duplicate-address-check
enabled
```

Related Documentation

- show aaa duplicate-address-check on page 306

Monitoring the Routing Table

Purpose Display the current state of the routing table, including routes not used for forwarding. An Access-P entry in the Type column of the output indicates routes that are downloaded by the RADIUS route-download server.

Action To display information in the routing table:

```
host1#show ip route
Protocol/Route type codes:
  I1- ISIS level 1, I2- ISIS level2,
  I- route type intra, IA- route type inter, E- route type external,
  i- metric type internal, e- metric type external,
  P- periodic download, O- OSPF, E1- external type 1, E2- external type2,
  N1- NSSA external type1, N2- NSSA external type2
  L- MPLS label, V- VRF, *- via indirect next-hop

Prefix/Length      Type       Next Hop      Dst/Met          Interface
------------------ ---------- --------------- ---------- -----------------
0.0.0.0/0          Static    10.13.10.1      1/0        FastEthernet6/0/0
192.168.10.0/23    Connect   10.13.10.187    0/0        FastEthernet6/0/0
192.168.21.21/32   Access-P  255.255.255.255 254/2      null0
192.168.22.22/32   Access-P  255.255.255.255 254/2      null0
```

```
192.168.23.23/32   Access-P  255.255.255.255 254/2      null0
192.168.24.24/32   Access-P  255.255.255.255 254/2      null0
```

Meaning Refer to the description of the **show ip route** command in *JunosE IP, IPv6, and IGP Configuration Guide* for additional information about the **show ip route** command.

Related Documentation

- show ip route on page 328

CHAPTER 29

Monitoring AAA Profiles and Subscriber Sessions

Monitoring AAA Profile Configuration

Purpose Display the configuration of all AAA profiles or of a specific profile.

Action To display the configuration of all AAA profiles or of a specific profile:

```
host1#show aaa profile name PreAuth1
preAuth1:
    atm nas-port-type: ADLSL-CAP
    ethernet nas-port-type: Cable
    profile-service-description: xyzService
    pre-authenticate
    allow xyz.com
    deny default
    translate xyz1.com abc.com
    aaaPerProfileName:aaaProfile1
    radiusPerProfileName:radiusProfile1
```

Meaning Table 19 on page 231 Lists the **show aaa profile** command output fields.

Table 19: show aaa profile Output Fields

Field Name	Field Description
atm nas-port-type	Configuration of NAS-Port-Type attribute for ATM interfaces
ethernet nas-port-type	Configuration of NAS-Port-Type attribute for Ethernet interfaces
profile-service-description	Description configured in the Service-Description attribute

Table 19: show aaa profile Output Fields *(continued)*

Field Name	Field Description
pre-authenticate	Indicates that subscriber preauthentication is configured for the profile
allow	One or more domain names that are allowed access to AAA authentication
deny	One or more domain names that are denied access to AAA authentication
translate	Original domain name and the name to which it is mapped for domain map lookup
aaaPerProfileName	Name of the AAA per-profile
radiusPerProfileName	Name of the RADIUS per-profile

Related Documentation

- show aaa profile on page 312

Monitoring the Number of Active Subscribers Per Port

Purpose Display the maximum number of active subscribers configured per port.

Action To display the maximum number of active subscribers configured per port:

```
host1#show aaa subscriber per-port-limit
     Subscriber Port Limits
     ----------------------
     Port              Limit
---------------   ---------------
0/2               5
0/3               2
3/2               2
```

Related Documentation

- show aaa subscriber per-port-limit on page 319

Monitoring the Maximum Number of Active Subscribers Per Virtual Router

Purpose Display the maximum number of active subscribers configured per virtual router.

Action To display the maximum number of active subscribers configured per virtual router:

```
host1# show aaa subscriber per-vr-limit
subscriber limit is 0
```

Related Documentation

- show aaa subscriber per-vr-limit on page 320

Monitoring Session Timeouts

Purpose Display idle and session timeouts.

Action To display idle and session timeouts:

```
host1#show aaa timeout
idle timeout 1200 seconds monitor ingress only
session timeout 3600 seconds
```

Related Documentation

- show aaa timeout on page 321

CHAPTER 30

Monitoring Route-Download Server Settings

Monitoring Statistics about the RADIUS Route-Download Server

Purpose Display statistics about the RADIUS route-download server configuration.

- Use the optional **statistics** keyword to display information about the RADIUS route download server operation.
- Use the optional **delta** keyword to show baselined statistics.

Action To display information about the RADIUS route-download server operation for IPv4 routes:

```
host1#show aaa route-download
AAA Route Downloader:     configured in virtual router default
Download Interval:        720 minutes
Retry Interval:           10 minutes
Default Cost:             2
Default Tag:              0
Base User Name:           <HOSTNAME>
Password:                 <DEFAULT>
Synchronization:          <NOT SET>

Status:                   idle
Last Download Attempt:    TUE DEC 19 22:46:47 2006
Last Download Success:    TUE DEC 19 22:46:47 2006
Last Regular Download:    complete
Next Download Scheduled:  WED DEC 20 10:46:47 2006
Next Regular Download:    WED DEC 20 10:46:47 2006
```

To display statistics about the RADIUS route-download server configuration for IPv4 routes:

```
host1#show aaa route-download statistics

Total Download Attempts: 2
Successful Downloads:    2
```

```
Downloaded Fragments:    3756
Downloaded Routes:       192000
IP Updates:              1
Updated Routes:          96000
Cleared Route Intervals: 0
```

To display information about the RADIUS route-download server operation for IPv6 routes:

```
host1#show aaa route-download ipv6
AAA Route Downloader:     configured in virtual router default
Download Interval:        720 minutes
Retry Interval:           10 minutes
Default Cost:             2
Default Tag:              0
Base User Name:           <HOSTNAME>
Password:                 <DEFAULT>
Synchronization:          <NOT SET>

Status:                   idle
Last Download Attempt:    TUE DEC 13 2011 00:05:43 UTC
Last Download Success:    TUE DEC 13 2011 00:05:43 UTC
Last Regular Download:    complete
Next Download Scheduled:  TUE DEC 13 2011 12:05:42 UTC
Next Regular Download:    TUE DEC 13 2011 12:05:42 UTC
```

To display statistics about the RADIUS route-download server configuration for IPv6 routes:

```
host1#show aaa route-download ipv6 statistics

Total Download Attempts: 3
Successful Downloads:    3
Downloaded Fragments:    30
Downloaded Routes:       240
IP Updates:              2
Updated Routes:          16
Cleared Route Intervals: 0
```

Meaning Table 20 on page 236 lists the **show aaa route-download** command and **show aaa route-download ipv6** command output fields.

Table 20: show aaa route-download Output Fields

Field Name	Field Description
AAA Route Downloader	Virtual router where the RADIUS route-download server is configured
Download Interval	Number of minutes between route downloads
Retry Interval	Number of minutes before retry after a download failure
Default Cost	Default cost of downloaded routes
Default Tag	Default tag for downloaded routes

Table 20: show aaa route-download Output Fields *(continued)*

Field Name	Field Description
Base User Name	Virtual router used for route-download requests; either <HOSTNAME> or the configured name
Password	Password for route-download requests or <DEFAULT>
Synchronization	Either <NOT SET> or the time that the server starts the route download operation each day
Status	Current status of route-download server; waiting for base router, waiting for IP warmstart, idle, downloading, updating ip, downloading and updating ip, or suspended
Last Download Attempt	Either <NEVER> or the day, date, and time of attempt
Last Download Success	Either <NEVER> or the day, date, and time of success
Last Regular Download	Status of last regular download; either complete or not complete
Next Download Scheduled	<DOWNLOAD ACTIVE>,<NOT SCHEDULED>, or the day, date, and time of next download
Next Regular Download	Day, date, and time
Total Download Attempts	Number of downloads attempted
Successful Downloads	Number of successful download operations
Downloaded Fragments	Number of downloaded fragments
Downloaded Routes	Number of downloaded routes
IP Updates	Number of IP updates
Updated Routes	Number of updated routes
Cleared Route Intervals	Number of cleared route intervals

Related Documentation

- show aaa route-download on page 313

Monitoring Routes Downloaded by the RADIUS Route-Download Server

Purpose Display information about the routes that are downloaded by the RADIUS route-download server.

Use the optional **detail** keyword to display more detailed information about the downloaded routes.

Action To display information about the IPv4 static routes that are downloaded by the RADIUS route-download server:

```
host1#show aaa route-download routes
96000 downloaded routes
```

To display detailed information about the IPv4 static routes that are downloaded by the RADIUS route-download server:

```
host1#show aaa route-download routes detail
Prefix/Length      Type        NextHop       Dst/Met  Intf   Tag
---------------  --------  ---------------  -------  -----  ---
192.168.1.1/32   Access-P  255.255.255.255  254/2    null0  0
192.168.1.5/32   Access-P  255.255.255.255  254/2    null0  0
192.168.1.9/32   Access-P  255.255.255.255  254/2    null0  0
192.168.1.13/32  Access-P  255.255.255.255  254/2    null0  0
192.168.1.17/32  Access-P  255.255.255.255  254/2    null0  0
192.168.1.21/32  Access-P  255.255.255.255  254/2    null0  0
```

To display information about the IPv6 routes that are downloaded by the RADIUS route-download server:

```
host1#show aaa route-download ipv6 routes
13 downloaded routes
```

To display detailed information about the IPv6 routes that are downloaded by the RADIUS route-download server:

```
host1#show aaa route-download ipv6 routes detail
Prefix/Length     Type     Dst/Met   Intf    Tag
-------------   --------   -------   -----   ---
f001::1/128     Access-P   0/2       null0   0
f002::1/128     Access-P   0/2       null0   0
f002::2/128     Access-P   0/2       null0   0
f002::3/128     Access-P   0/2       null0   0
f002::4/128     Access-P   0/2       null0   0
f003::2/128     Access-P   0/2       null0   0
f004::2/128     Access-P   0/2       null0   0
f005::2/128     Access-P   0/2       null0   0
f006::2/128     Access-P   0/2       null0   0
f007::2/128     Access-P   0/2       null0   0
f008::2/128     Access-P   0/2       null0   0
f009::2/128     Access-P   0/2       null0   0
f00a::2/128     Access-P   0/2       null0   0
```

Meaning Table 21 on page 238 lists the **show aaa route-download routes** command and **show aaa route-download ipv6 routes** command output fields.

Table 21: show aaa route-download routes Output Fields

Field Name	Field Description
downloaded routes	Number of current downloaded routes
Prefix/Length	IP address prefix and mask information for downloaded routes

Table 21: show aaa route-download routes Output Fields *(continued)*

Field Name	Field Description
Type	Type of downloaded routes; Access-P indicates routes downloaded from the RADIUS route-download server
NextHop	IP address of the next hop
Dst/Met	Administrative distance and number of hops for the route
Tag	Tag assigned to downloaded routes
Intf	Interface type and specifier

Related Documentation

- show aaa route-download routes on page 314
- show aaa route-download ipv6 routes on page 315

Monitoring Chassis-Wide Routes Downloaded by the RADIUS Route-Download Server

Purpose Display chassis-wide information about routes that are downloaded by RADIUS route-download servers.

Use the optional **detail** keyword to display more detailed information about the downloaded routes.

Use the optional **start** keyword to specify the first router context that you want to display in the output. For example, aaa:a2 specifies that the display shows a list of router contexts starting with VRF a2 in virtual router aaa.

Action To display chassis-wide information about IPv4 routes that are downloaded by RADIUS route-download servers:

```
host1#show aaa route-download routes global
                                                  Number
                                                    of
Virtual Router        VRF       Present Routes
--------------- --------------- ------- ------
aaa                             n       4
aaa             a1              n       4
default                         y       4
default         d1              n       4
```

To display more detailed information about the downloaded IPv4 routes:

```
host1# show aaa route-download routes global detail

Virtual Router   VRF  Present  Prefix/Length      Type       NextHop       Dst/Met  Intf   Tag
---------------  ---  -------  ---------------  --------  ---------------  -------  -----  ---
aaa                   n        192.168.1.1/32   Access-P  255.255.255.255  0/2      null0  0
aaa                   n        192.168.1.2/32   Access-P  255.255.255.255  0/2      null0  0
aaa                   n        192.168.3.1/32   Access-P  255.255.255.255  0/2      null0  0
```

```
aaa                  n        192.168.4.1/32   Access-P  255.255.255.255  0/2      null0  0
aaa             a1   n        192.168.5.3/32   Access-P  255.255.255.255  0/2      null0  0
aaa             a1   n        192.168.7.1/32   Access-P  255.255.255.255  0/2      null0  0
aaa             a1   n        192.168.7.5/32   Access-P  255.255.255.255  0/2      null0  0
aaa             a1   n        192.168.9.1/32   Access-P  255.255.255.255  0/2      null0  0
default              y        192.168.22.1/32  Access-P  255.255.255.255  0/2      null0  0
default              y        192.168.23.1/32  Access-P  255.255.255.255  0/2      null0  0
default              y        192.168.24.1/32  Access-P  255.255.255.255  0/2      null0  0
default              y        192.168.25.1/32  Access-P  255.255.255.255  0/2      null0  0
default         d1   n        192.168.40.6/32  Access-P  255.255.255.255  0/2      null0  0
default         d1   n        192.168.40.7/32  Access-P  255.255.255.255  0/2      null0  0
default         d1   n        192.168.40.8/32  Access-P  255.255.255.255  0/2      null0  0
default         d1   n        192.168.40.9/32  Access-P  255.255.255.255  0/2      null0  0
```

To specify the first router context that you want to display in the output:

```
host1#show aaa route-download routes global start aaa:a2
                                                Number
                                                  of
Virtual Router        VRF       Present Routes
--------------- --------------- ------- ------
default                         y       4
default         d1              n       4
```

To display chassis-wide information about IPv6 routes that are downloaded by RADIUS route-download servers:

```
host1#show aaa route-download ipv6 routes global
                                                Number
                                                  of
Virtual Router        VRF       Present Routes
--------------- --------------- ------- ------
def                             y       3
def             temp            y       1
default                         y       13
Context1                        n       27
test                            n       36
```

To display more detailed information about the downloaded IPv6 routes:

```
host1# show aaa route-download ipv6 routes global detail
Virtual
Router    VRF    Present   Prefix/Length     Type     Dst/Met   Intf    Tag
-------   ----   -------   -------------   --------   -------   -----   ---
def               y         f00b::2/128     Access-P   0/2       null0   0
def               y         f00b::3/128     Access-P   0/2       null0   0
def               y         f00b::4/128     Access-P   0/2       null0   0
def       temp    y         f00b::1/128     Access-P   0/2       null0   0
default           y         f001::1/128     Access-P   0/2       null0   0
default           y         f002::1/128     Access-P   0/2       null0   0
default           y         f002::2/128     Access-P   0/2       null0   0
default           y         f002::3/128     Access-P   0/2       null0   0
default           y         f002::4/128     Access-P   0/2       null0   0
default           y         f003::2/128     Access-P   0/2       null0   0
default           y         f004::2/128     Access-P   0/2       null0   0
default           y         f005::2/128     Access-P   0/2       null0   0
default           y         f006::2/128     Access-P   0/2       null0   0
default           y         f007::2/128     Access-P   0/2       null0   0
```

To specify the router context that you want to display in the output:

```
host1#show aaa route-download ipv6 routes global start Context1
                                          Number
                                            of
Virtual Router        VRF       Present Routes
--------------- --------------- ------- ------
Context1                        n       27
test                            n       36
```

Meaning Table 22 on page 241 lists the **show aaa route-download routes global** command and **show aaa route-download ipv6 routes global** command output fields.

Table 22: show aaa route-download routes global Output Fields

Field Name	Field Description
Virtual Router	Name of the virtual router used to download the routes
VRF	Name of the VRF used to download the routes
Present	Routes have been downloaded; y (yes) or n (no) indicates if the router context has been created.
Number of Routes	Number of current downloaded routes
Prefix/Length	IP address prefix and mask information for downloaded routes
Type	Type of downloaded routes; Access-P indicates routes downloaded from the RADIUS route-download server
NextHop	IP address of the next hop
Dst/Met	Administrative distance and number of hops for the route
Tag	Tag assigned to downloaded routes
Intf	Interface type and specifier

Related Documentation

- show aaa route-download routes global on page 316
- show aaa route-download ipv6 routes global on page 317

CHAPTER 31

Monitoring AAA Accounting Details

Monitoring AAA Statistics

Purpose Display authentication, authorization, and accounting statistics.

Use the optional **delta** keyword to specify that baselined statistics are to be shown.

Action To display authentication, authorization, and accounting statistics:

```
host1#show aaa statistics
```

```
               AAA Statistics
               --------------
             Statistic                 Count
-----------------------------------    -----
incoming initiate requests             109
incoming disconnect requests           7
outgoing grant (tunnel) responses      3
outgoing grant responses               6
outgoing deny responses                0
outgoing error responses               0
outgoing Authentication requests       9
incoming Authentication responses      9
outgoing Re-Authentication requests    0
incoming Re-Authentication responses   0
outgoing Pre-Authentication requests   1
incoming Pre-Authentication responses  1
outgoing Accounting requests           120
incoming Accounting responses          120
outgoing Duplicate Acct requests       18
incoming Duplicate Acct responses      18
outgoing Broadcast Acct requests       32
incoming Broadcast Acct responses      32
outgoing Address requests              0
incoming Address responses             0
```

Meaning Table 23 on page 244 lists the **show aaa statistics** command output fields.

Table 23: show aaa statistics Output Fields

Field Name	Field Description
incoming initiate requests	Number of incoming AAA requests (from other E Series applications) for user connect services
incoming disconnect requests	Number of incoming AAA requests (from other E Series applications) for user disconnect services
outgoing grant (tunnel) responses	Number of outgoing tunnel grant responses to AAA requests
outgoing grant responses	Number of outgoing grant responses to AAA requests
outgoing deny responses	Number of outgoing deny responses to AAA requests
outgoing error responses	Number of outgoing error responses to AAA requests
outgoing Authentication requests	Number of authentication requests from AAA to the authentication task
incoming Authentication responses	Number of authentication responses from the authentication task to AAA
outgoing Re-Authentication requests	Number of reauthentication requests from AAA to the authentication task
incoming Re-Authentication responses	Number of reauthentication responses from the authentication task to AAA
outgoing Pre-Authentication requests	Number of preauthentication requests from AAA to the preauthentication task
incoming Pre-Authentication responses	Number of preauthentication responses from the preauthentication task to AAA
outgoing Accounting requests	Number of accounting requests (starts, updates, stops) from AAA to the accounting task
incoming Accounting responses	Number of accounting responses (starts, updates, stops) from the accounting task to AAA
outgoing Duplicate Acct requests	Number of duplicate accounting requests (starts, updates, stops) from AAA to the accounting task
incoming Duplicate Acct responses	Number of duplicate accounting responses (starts, updates, stops) from the accounting task to AAA
outgoing Broadcast Acct requests	Number of broadcast accounting requests (starts, updates, stops) from AAA to the accounting task
incoming Broadcast Acct responses	Number of broadcast accounting responses (starts, updates, stops) from the accounting task to AAA

Table 23: show aaa statistics Output Fields *(continued)*

Field Name	Field Description
outgoing Address requests	Number of address allocation/release requests from AAA to address allocation task
incoming Address responses	Number of address allocation/release responses from the address allocation task to AAA

Related Documentation

- show aaa statistics on page 318

Monitoring Interim Accounting for Users on the Virtual Router

Purpose Display the default interval used for interim accounting for users on the virtual router. An entry of 0 indicates that the feature is disabled.

Action To display the default interval used for interim accounting for users on the virtual router:

```
host1:vrXyz7#show aaa user accounting interval
user-acct-interval 20
```

Related Documentation

- show aaa user accounting interval on page 322

Monitoring Virtual Router Groups Configured for AAA Broadcast Accounting

Purpose Display the virtual router groups that are configured for AAA broadcast accounting.

For additional information about the **show configuration** command, see *JunosE System Basics Configuration Guide*.

Action To display the virtual router groups that are configured for AAA broadcast accounting:

```
host1#show configuration category aaa global-attributes
! Configuration script being generated on MON JAN 10 2005 15:19:19 UTC
! Juniper Edge Routing Switch ERX1440
! Version: 9.9.9 development-4.0 (January 7, 2005  17:26)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE:  This script represents only a subset of the full system configuration.
! The category displayed is: aaa global-attributes
!
aaa accounting vr-group groupXyzCompany10
 aaa virtual-router 1 vrXyzA
 aaa virtual-router 2 vrXyzB
 aaa virtual-router 3 vrXyzC
 aaa virtual-router 4 vrXyzD

aaa accounting vr-group groupXyzCompany20
 aaa virtual-router 1 vrXyzP
 aaa virtual-router 2 vrXyzQ
 aaa virtual-router 3 vrXyzR
```

```
 aaa virtual-router 4 vrXyzS
!
hostname "host1"
```

Meaning Table 24 on page 246 lists the **show configuration category aaa global-attributes** command output fields.

Table 24: show configuration category aaa global-attributes Output Fields

Field Name	Field Description
aaa accounting vr-group	Name of virtual router groups
aaa virtual-router	Name and index number of the virtual routers that are members of the virtual router group

Related Documentation

- show configuration

CHAPTER 32

Monitoring COPS Layer Settings

Monitoring the COPS Layer Over SRC Connection

Purpose Display information about the COPS layer over which the SRC connection is made.

Action To display information about the COPS layer over which the SRC connection is made:

```
host1#show cops info
General Cops Information:

        Sessions Created: 1
        Sessions Deleted: 0
        Current Sessions: 1
        Bytes Received: 680
        Packets Received: 17
        Bytes Sent: 692
        Packets Sent: 21
        Keep Alive Received: 12
        Keep Alive Sent: 12

Session Information
        Remote Ip Address: 10.10.0.223
        Remote TCP Port: 4001
        Client Type: 16384
        Bytes Received:   2224
        Packets Received: 5
        Bytes Sent:       596
        Packets Sent:     9
        REQ Sent:         4
        DEC Rcv:          4
        RPT Sent:         4
        DRQ Sent:         0
        SSQ Rcv:          0
        OPN Sent:         1
        CAT Rcv:          1
        CC Sent:          0
        CC Rcv:           0
        SSC Sent:         0
```

Meaning Table 25 on page 248 lists the **show cops info** command output fields.

Table 25: show cops info Output Fields

Field Name	Field Description
Session Created	Number of COPS sessions created
Sessions Deleted	Number of COPS sessions deleted
Current Sessions	Number of current COPS sessions
Bytes Received	Number of bytes received on all COPS sessions
Packets Received	Number of packets received on all COPS sessions
Bytes Sent	Number of bytes transmitted on all COPS sessions
Packets Sent	Number of packets transmitted on all COPS sessions
Keep Alive Received	Number of COPS keepalive messages received
Keep Alive Sent	Number of COPS keepalive messages *sent*
Remote IP Address	IP address of the remote pee
Remote TCP Port	TCP port number of the remote peer
Client Type	Type of client for the session. For this release the client type must be 16640 (SRC client).
Bytes Received	Number of bytes received for this COPS session
Packets Received	Number of packets received for this COPS session
Bytes Sent	Number of bytes sent on this COPS session
Packets Sent	Number of packets sent on this COPS session
REQ Sent	Number of Request packets sent on this COPS session
DEC Rcv	Number of Decision packets received on this COPS session
RPT Sent	Number of Report packets sent on this COPS session
DRQ Sent	Number of Delete Requests sent on this COPS session
SSQ Rcv	Number of Synch Requests received on this COPS session
OPN Sent	Number of Open messages sent on this COPS session

Table 25: show cops info Output Fields *(continued)*

Field Name	Field Description
CAT Rcv	Number of Client Accepts packets received on this COPS session
CC Sent	Number of Client Closes packets sent on this COPS session
CC Rcv	Number of Client Closes packets received on this COPS session
SSC Sent	Number of Sync Complete packets sent on this COPS session

Related Documentation

- show cops info on page 323

Monitoring Statistics About the COPS Layer

Purpose Display statistics about the COPS layer over which the SRC connection is made.

Action To display statistics about the COPS layer:

```
host1#show cops statistics
General Cops Information:
        Sessions Created: 0
        Sessions Deleted: 0
        Current Sessions: 0
        Bytes Received: 1108
        Packets Received: 12
        Bytes Sent: 1572
        Packets Sent: 18
        Keep Alive Received: 2
        Keep Alive Sent: 2
Session Information:
        Client Type: 24754
        Bytes Received:   2539032
        Packets Received: 20388
        Bytes Sent:       4386648
        Packets Sent:     51337
        REQ Sent:         21203
        DEC Rcv:          20388
        RPT Sent:         20391
        DRQ Sent:         9743
        SSQ Rcv:          0
        OPN Sent:         0
        CAT Rcv:          0
        CC Sent:          0
        CC Rcv:           0
        SSC Sent:         0
```

Meaning Table 26 on page 250 lists the **show cops statistics** command output fields.

Table 26: show cops statistics Output Fields

Field Name	Field Description
Session Created	Number of COPS sessions created
Sessions Deleted	Number of COPS sessions deleted
Current Sessions	Number of current COPS sessions
Bytes Received	Number of bytes received on all COPS sessions
Packets Received	Number of packets received on all COPS sessions
Bytes Sent	Number of bytes transmitted on all COPS sessions
Packets Sent	Number of packets transmitted on all COPS sessions
Keep Alive Received	Number of COPS keepalive messages received
Keep Alive Sent	Number of COPS keepalive messages *sent*
Client Type	Type of client for the session
Bytes Received	Number of bytes received for this COPS session
Packets Received	Number of packets received for this COPS session
Bytes Sent	Number of bytes sent on this COPS session
Packets Sent	Number of packets sent on this COPS session
REQ Sent	Number of Request packets sent on this COPS session
DEC Rcv	Number of Decision packets received on this COPS session
RPT Sent	Number of Report packets sent on this COPS session
DRQ Sent	Number of Delete Requests sent on this COPS session
SSQ Rcv	Number of Synch Requests received on this COPS session
OPN Sent	Number of Open messages sent on this COPS session
CAT Rcv	Number of Client Accepts packets received on this COPS session
CC Sent	Number of Client Closes packets sent on this COPS session

Table 26: show cops statistics Output Fields *(continued)*

Field Name	Field Description
CC Rcv	Number of Client Closes packets received on this COPS session
SSC Sent	Number of Sync Complete packets sent on this COPS session

Related Documentation

- show cops statistics on page 324

CHAPTER 33

Monitoring SRC Client Settings

Monitoring SRC Client Connection Status

Purpose Display the current status of the SRC client connection to the SAEs. The command output refers to the SRC client by its former name, SSC client.

Action To display the status of the SRC client connection:

```
host1#show sscc info
The SSC Client configured protocols : IP(v4), DHCP(v4), L2TP(LAC)
The SSC Client is currently unconnected
The SSC Client configured servers are:
        Primary: 10.10.2.2:3
        Secondary: 0.0.0.0:0
        Tertiary: 0.0.0.0:0
        Local Source: FastEthernet 0/0, Local Source Address: 10.13.5.61
        The configured transport router is: default
        The configured retry timer is (seconds): 90
        The configured update-policy-request is: Enabled
        The connection state is: NoConnection
 SSC Client Statistics:
        Policy Commands received   0
        Policy Commands(List)      0
        Policy Commands(Acct)      0
        Bad Policy Cmds received   0
        Error Policy Cmds received 0
        Policy Reports sent        0
        Connection Open requests   0
        Connection Open completed  0
        Connection Closed sent     0
        Connection Closed remotely 0
        Create Interfaces sent     0
        Delete Interfaces sent     0
        Active IP Interfaces       2
        IP Interface Transitions   0
        Synchronizes received      0
        Synchronize Complete sent  0
        Internal Errors            0
        Communication Errors       0
```

```
Tokens Seen                0
Active Tokens              0
Token Transitions          0
Token Creates Sent         0
Token Deletes Sent         0
Active Addresses           0
Address Transitions        0
Create Addresses Sent      0
Delete Addresses Sent      0
Authentication Successes   0
Authentication Failures    0
```

Meaning Table 27 on page 254 lists the **show sscc info** command output fields.

Table 27: show sscc info Output Fields

Field Name	Field Description
The SSC client configured protocols	Protocols that are enabled on the virtual router for policy and QoS management by the SRC software
The SSC client configured servers	IP addresses of the primary, secondary, and tertiary SAEs
Local Source	Fixed source interface for the TCP/COPS connection
Local Source Address	Fixed source address for the TCP/COPS connection
The configured transport router is	Router on which is TCP/COPS connection is established
The configured retry timer is (seconds)	Delay period the client waits for a response from the SAE before submitting request again
The configured update-policy-request is	Whether the router or the SRC client retrieves DSL line rate parameters, whenever the values change after connection establishment, from ANCP and transfers the details to the COPS server with other COPS messages, enabled or disabled
The connection state is	Current state of the TCP/COPS connection

Table 27: show sscc info Output Fields *(continued)*

Field Name	Field Description
SSC Client Statistics	Statistics about the connection between the SRC client and SAE • Policy Commands received—Number of policy commands received on the SRC client connection • Policy Commands(List)—Number of Policy Commands with subtype List • Policy Commands(Acct)—Number of Policy Commands with subtype Accounting • Bad Policy Cmds received—Number of Policy Commands received with bad policies • Error Policy Cmds received—Number of Policy Commands received with errors • Policy Reports sent—Number of Policy Reports sent • Connection Open requests—Number of connections the SRC client has tried to open with a remote SAE • Connection Open completed—Number of connections successfully open to the SAE • Connection Closed sent—Number of connections the SRC client has closed • Connection Closed remotely—Number of connections that were closed by the remote SAE • Create Interfaces sent—Number of create interface indications sent to the SAE • Delete Interfaces sent—Number of delete interface indications sent to the SAE • Active IP Interfaces—Current number of active IP interfaces the SRC client is aware of • IP Interface Transitions—Number of IP interface transitions logged by the SRC client • Synchronizes received—Number of synchronization requests the SRC client received from the SAE • Synchronize Complete sent—Number of synchronization complete indications sent • Internal Errors—Number of internal errors • Communication Errors—Number of errors with lower-layer communications (such as socket errors)

Related Documentation

- show sscc info on page 339

Monitoring SRC Client Connection Statistics

Purpose Display statistics about connection between the SRC client and SAE. The command output refers to the SRC client by its former name, SSC client.

Action To display statistics for the SRC client connection:

```
host1#show sscc statistics
SSC Client Statistics:
```

```
Policy Commands received   0
Policy Commands(List)      0
Policy Commands(Acct)      0
Bad Policy Cmds received   0
Error Policy Cmds received 0
Policy Reports sent        3
Connection attempts        7
Connection Open requests   7
Connection Open completed  0
Connection Closed sent     0
Connection Closed remotely 5
Create Interfaces sent     0
Delete Interfaces sent     3
Active IP Interfaces       3282
IP Interface Transitions   3281
Synchronizes received      0
Synchronizes rcvd & dropped 0
Synchronize Complete sent  2
Internal Errors            0
Communication Errors       0
Discovers Seen             15263
Active Discovers           4911
Discover Transitions       20704
Discover Creates Sent      15263
Discover Deletes Sent      10352
Active Addresses           3274
Address Transitions        3280
Create Addresses Sent      3277
Delete Addresses Sent      3
```

Meaning Table 28 on page 256 lists the **show sscc statistics** command output fields.

Table 28: show sscc statistics Output Fields

Field Name	Field Description
Policy Commands received	Number of policy commands received on the SRC client connection
Policy Commands(List)	Number of Policy Commands with subtype List
Policy Commands(Acct)	Number of Policy Commands with subtype Accounting
Bad Policy Cmds received	Number of Policy Commands received with bad policies
Error Policy Cmds received	Number of Policy Commands received with errors
Policy Reports sent	Number of Policy Reports sent
Connection Open requests	Number of connections the SRC client has tried to open with a remote SAE
Connection Open completed	Number of connections successfully open to the SAE
Connection Closed sent	Number of connections the SRC client has closed

Table 28: show sscc statistics Output Fields *(continued)*

Field Name	Field Description
Connection Closed remotely	Number of connections that were closed by the remote SAE
Create Interfaces sent	Number of create interface indications sent to the SAE
Delete Interfaces sent	Number of delete interface indications sent to the SAE
Active IP Interfaces	Current number of active IP interfaces the SRC client is aware of
IP Interface Transitions	Number of IP interface transitions logged by the SRC client
Synchronizes received	Number of synchronization requests the SRC client received from the SAE
Synchronize Complete sent	Number of synchronization complete indications sent
Internal Errors	Number of internal errors
Communication Errors	Number of errors with lower-layer communications (such as socket errors)

Related Documentation

- show sscc statistics on page 341

Monitoring SRC Client Connection Statistics

Purpose Display statistics about connection between the SRC client and SAE. The command output refers to the SRC client by its former name, SSC client.

Action To display statistics for the SRC client connection:

```
host1#show sscc statistics
SSC Client Statistics:
        Policy Commands received   0
        Policy Commands(List)      0
        Policy Commands(Acct)      0
        Bad Policy Cmds received   0
        Error Policy Cmds received 0
        Policy Reports sent        3
        Connection attempts        7
        Connection Open requests   7
        Connection Open completed  0
        Connection Closed sent     0
        Connection Closed remotely 5
        Create Interfaces sent     0
        Delete Interfaces sent     3
```

```
Active IP Interfaces       3282
IP Interface Transitions   3281
Synchronizes received      0
Synchronizes rcvd & dropped 0
Synchronize Complete sent  2
Internal Errors            0
Communication Errors       0
Discovers Seen             15263
Active Discovers           4911
Discover Transitions       20704
Discover Creates Sent      15263
Discover Deletes Sent      10352
Active Addresses           3274
Address Transitions        3280
Create Addresses Sent      3277
Delete Addresses Sent      3
```

Meaning Table 28 on page 256 lists the **show sscc statistics** command output fields.

Table 29: show sscc statistics Output Fields

Field Name	Field Description
Policy Commands received	Number of policy commands received on the SRC client connection
Policy Commands(List)	Number of Policy Commands with subtype List
Policy Commands(Acct)	Number of Policy Commands with subtype Accounting
Bad Policy Cmds received	Number of Policy Commands received with bad policies
Error Policy Cmds received	Number of Policy Commands received with errors
Policy Reports sent	Number of Policy Reports sent
Connection Open requests	Number of connections the SRC client has tried to open with a remote SAE
Connection Open completed	Number of connections successfully open to the SAE
Connection Closed sent	Number of connections the SRC client has closed
Connection Closed remotely	Number of connections that were closed by the remote SAE
Create Interfaces sent	Number of create interface indications sent to the SAE
Delete Interfaces sent	Number of delete interface indications sent to the SAE

Table 29: show sscc statistics Output Fields *(continued)*

Field Name	Field Description
Active IP Interfaces	Current number of active IP interfaces the SRC client is aware of
IP Interface Transitions	Number of IP interface transitions logged by the SRC client
Synchronizes received	Number of synchronization requests the SRC client received from the SAE
Synchronize Complete sent	Number of synchronization complete indications sent
Internal Errors	Number of internal errors
Communication Errors	Number of errors with lower-layer communications (such as socket errors)

Related Documentation

- show sscc statistics on page 341

Monitoring the SRC Client Version Number

Purpose Display the SRC client (formerly SDX client) version number.

Action To display the SRC client version number:

```
host1#show sscc version
The SSC Client version is: 4.0
```

Related Documentation

- show sscc version on page 342

CHAPTER 34

Monitoring the IP Local Address Pools Configuration

Monitoring Local Address Pools

Purpose Display information about the local address pools configured on your router. If you do not specify the name of a local address pool, the router displays all local address pools.

Action To display information about local address pools:

```
host1#show ip local pool

         High    Abated
Pool    Thresh   Thresh   Trap   Group
-----   ------   ------   ----   -----
poolA       85       75    N

     Aliases
     -------
      alias1
                                  In
      Begin        End      Free   Use
     --------   ---------   ----   ---
     10.1.1.1   10.1.1.10    10     0
     10.1.2.1   10.1.2.10    10     0
     10.1.3.1   10.1.3.10    10     0

         High    Abated
Pool    Thresh   Thresh   Trap   Group
-----   ------   ------   ----   -----
poolB       85       75    N

     Aliases
     -------
      alias2
                                  In
      Begin        End      Free   Use
     --------   ---------   ----   ---
     10.2.1.1   10.2.1.10    10     0
     10.2.2.1   10.2.2.10    10     0
```

```
          High    Abated
Pool     Thresh   Thresh   Trap   Group
-----    ------   ------   ----   -----
poolC        85       75    N

     Aliases
     -------
      alias3
                                    In
      Begin         End       Free  Use
     --------   ---------    ----   ---
     10.3.1.1   10.3.1.10     10     0

          High    Abated
Pool     Thresh   Thresh   Trap   Group
-----    ------   ------   ----   -----
poolD        85       75    N

     Aliases
     -------
       poolA
       poolB
       poolC
                                    In
      Begin         End       Free  Use
     --------   ----------    ----   ---
     10.4.1.1   10.4.1.255    255     0
```

Meaning Table 30 on page 262 lists the **show ip local pool** command output fields.

Table 30: show ip local pool Output Fields

Field Name	Field Description
Pool	User-specified name of the address pool
High Thresh	High utilization threshold value
Abated Thresh	Abated utilization threshold value
Trap	Enable SNMP pool utilization traps: Y (yes) or N (no)
Aliases	Aliases for the local address pool
Begin	Starting IP address
End	Ending IP address
Free	Number of addresses available for use
In Use	Number of addresses currently in use

Related Documentation

- show ip local pool on page 326

Monitoring Local Address Pool Aliases

Purpose Display information about aliases for the local address pools configured on your router. If you do not specify a particular alias, the router displays all aliases.

Action To display information about local address pool aliases:

```
host1#show ip local alias

Alias    Pool
------   -----
alias1   poolA
alias2   poolB
alias3   poolC
 poolA   poolD
 poolB   poolD
 poolC   poolD
```

Meaning Table 31 on page 263 lists the show **ip local alias** command output fields.

Table 31: show ip local alias Output Fields

Field Name	Field Description
Alias	Name of alias for the local address pool
Pool	Name of the local address pool

Related Documentation

- show ip local alias on page 325

Monitoring Local Address Pool Statistics

Purpose Display local address pool statistics. Use the optional **delta** keyword to specify that baselined statistics are to be shown.

Action To display local address pool statistics:

```
host1#show ip local pool statistics
 Local Address Pool Statistics

            Statistic               Values
--------------------------------   ------
Requests denied (pool exhaustion)   0
```

Related Documentation

- show ip local pool on page 326

Monitoring Shared Local Address Pools

Purpose Display the shared local address pool configurations.

Action To display shared local address pool configuration information:

```
host1#show ip local shared-pool

Shared Pool   In Use  Dhcp Pool
-----------   ------  ---------
shared_poolA  253     dhcp_pool_25
shared_poolB  83      dhcp_pool_25
shared_poolC  99      dhcp_pool_17
```

Meaning Table 32 on page 264 lists the **show ip local shared-pool** command output fields.

Table 32: show ip local shared-pool Output Fields

Field Name	Field Description
Shared Pool	Name of the shared local address pool
In Use	Number of addresses allocated
Dhcp Pool	Name of the DHCP address pool

Related Documentation

- show ip local shared-pool on page 327

CHAPTER 35

Monitoring RADIUS Servers and Services for AAA Features

Monitoring the RADIUS Server Algorithm

Purpose Display information about the currently configured RADIUS server algorithm.

Action To display the RADIUS server algorithm:

```
host1#show radius algorithm
direct
```

Related Documentation

- show radius algorithm on page 333

Monitoring the RADIUS Attribute Used for DHCPv6 Prefix Delegation

Purpose Display the RADIUS attribute used for DHCPv6 Prefix Delegation.

Action To display the RADIUS attribute used for DHCPv6 Prefix Delegation:

```
host1#show aaa dhcpv6-delegated-prefix
DHCPv6 Delegated Prefix : Framed-IPv6-Prefix
```

Related Documentation
- show aaa dhcpv6-delegated-prefix on page 309

Monitoring the RADIUS Attribute Used for IPv6 Neighbor Discovery Router Advertisements

Purpose Display the RADIUS attribute used for IPv6 Neighbor Discovery router advertisements.

Action To display the RADIUS attribute used for IPv6 Neighbor Discovery router advertisements:

```
host1#show aaa ipv6-nd-ra-prefix
IPv6 ND RA Prefix       : IPv6-NdRa-Prefix (Juniper VSA)
```

Related Documentation
- show aaa ipv6-nd-ra-prefix on page 308

Monitoring the RADIUS Rollover Configuration

Purpose Display the configuration of the RADIUS rollover-on-reject feature.

Action To display the RADIUS rollover configuration:

```
host1#show radius rollover-on-reject
rollover-on-reject enabled
```

Meaning RADIUS rollover-on-reject is enabled.

Related Documentation
- show radius rollover-on-reject on page 335

Monitoring RADIUS Override Settings

Purpose Display the current RADIUS override settings.

Action To display the RADIUS override settings:

```
host1:vrXyz7#show radius override
nas-ip-addr: nas-ip-addr
nas-info:    from authentication virtual router
```

Meaning Table 33 on page 266 lists the **show radius override** command output fields.

Table 33: show radius override Output Fields

Field Name	Field Description
nas-ip-addr	Either the NAS-IP-Address [4] attribute is used, or it is overridden with the Tunnel-Client-Endpoint [66] attribute.
nas-info	Either the NAS-IP-Address [4] and NAS-Identifier [32] attributes of the virtual router generating the accounting information are used, or they are overridden with the respective attributes of the authentication virtual router.

Related Documentation

- show radius override on page 334

Monitoring RADIUS Server Information

Purpose Display RADIUS server information.

Use with the optional **accounting**, **authentication**, **dynamic-request**, **route-download**, or **pre-authentication** keywords to limit output to the specific type of server.

Action To display RADIUS server configuration information:

```
host1#show radius servers
                RADIUS Authentication Configuration
                -----------------------------------
                 Udp    Retry             Maximum    Dead
 IP Address      Port   Count   Timeout   Sessions   Time   Secret  Status
 -------------   ----   -----   -------   --------   ----  ------  ------
 172.28.30.117   1812   3         3         255      30     radius  dead
 172.28.30.118   1812   3         3         255      30     radius  active
 172.28.30.119   1812   3         3         255      30     radius  alive

                  RADIUS Accounting Configuration
                  -------------------------------
                 Udp    Retry             Maximum    Dead
 IP Address      Port   Count   Timeout   Sessions   Time   Secret  Status
 -------------   ----   -----   -------   --------   ----   ------  ------
 172.28.30.117   1813   3       3         255        30     radius  dead
 172.28.30.118   1813   3       3         255        30     radius  active
 172.28.30.119   1813   3       3         255        30     radius  alive

                RADIUS Pre-Authentication Configuration
                --------------------------------------
                 Udp    Retry             Maximum    Dead
 IP Address      Port   Count   Timeout   Sessions   Time   Secret  Status
-------------   ----   -----   -------   --------   ----   ------  ------
 172.28.30.117   1812   3       3         255        30     radius  dead
 172.28.30.118   1812   3       3         255        30     radius  active
 172.28.30.119   1812   3       3         255        30     radius  alive

                RADIUS Route-Download Configuration
                -----------------------------------
                 Udp    Retry             Maximum    Dead
 IP Address      Port   Count   Timeout   Sessions   Time   Secret  Status
-------------   ----   -----   -------   --------   ----   ------  ------
192.168.30.16   1812   3       3         255        30     radius  dead
192.168.30.17   1812   3       3         255        30     radius  active
192.168.30.18   1812   3       3         255        30     radius  alive
```

Meaning If a RADIUS server was never configured on the virtual router, the command displays the following message:

```
host1#show radius servers
no radius servers configured
```

If a RADIUS server was configured previously and then removed on the virtual router, the command displays the following information:

```
host1#show radius servers
                RADIUS Authentication Configuration
```

```
                 ------------------------------------
                  Udp    Retry             Maximum    Dead
 IP Address       Port   Count   Timeout   Sessions   Time   Secret  Status
 -------------    ----    -----   -------   --------  ----  ------  ------

                   RADIUS Accounting Configuration
                   -------------------------------
                  Udp    Retry             Maximum    Dead
 IP Address       Port   Count   Timeout   Sessions   Time   Secret  Status
 -------------   ----   -----   -------  --------   ----    ------  ------

                RADIUS Pre-Authentication Configuration
                ---------------------------------------
                  Udp    Retry             Maximum    Dead
 IP Address       Port   Count   Timeout   Sessions   Time   Secret  Status
-------------    ----   -----   -------   --------  ----   ------  ------

                RADIUS Route-Download Configuration
                -----------------------------------
                  Udp    Retry             Maximum    Dead
 IP Address       Port   Count   Timeout   Sessions   Time   Secret  Status
-------------    ----   -----   -------   --------   ----   ------  ------
```

Table 34 on page 268 lists the **show radius servers** command output fields.

Table 34: show radius servers Output Fields

Field Name	Field Description
IP Address	IP address of RADIUS server
Udp Port	Number of the UDP port of the RADIUS server
Retry Count	Maximum number of times that the router retransmits a RADIUS packet to the RADIUS server
Timeout	Interval (in seconds) before the router retransmits a RADIUS packet to the RADIUS server
Maximum Sessions	Number of outstanding requests to the RADIUS server
Dead Time	Amount of time to remove the authentication server or accounting server from the available list when a timeout occurs
Secret	Configured authentication server or accounting server secret

Table 34: show radius servers Output Fields *(continued)*

Field Name	Field Description
Status	Status of the configured RADIUS server: • dead-The status displayed if the server does not respond within the configured number of retransmit counts, and if Dead Time is configured to a non-zero value. • active-The status displayed of the earliest configured, non-dead server if the server is accessed using the direct algorithm. The status displayed of all non-dead servers if the server is accessed using the round-robin algorithm. • alive-The status displayed of all non-dead servers except the earliest configured non-dead server, if the server is accessed using the direct algorithm. The status of none of the servers if the server is accessed using the round-robin algorithm.

Related Documentation
- show radius servers on page 336

Monitoring RADIUS Accounting for L2TP Tunnels

Purpose Display the status for RADIUS accounting for L2TP tunnels.

Action To display RADIUS accounting for L2TP tunnels:

```
host1#show radius tunnel-accounting
disabled
```

Meaning RADIUS accounting is either enabled or disabled.

Related Documentation
- show radius tunnel-accounting on page 338

Monitoring RADIUS Services Statistics

Purpose Use to display statistics for RADIUS services.

Use with the optional **accounting**, **authentication**, **dynamic-request**, **route-download**, or **pre-authentication** keywords to limit output to the specific type of statistics. Use the optional **delta** keyword to specify that baselined statistics are to be shown.

Action To display RADIUS authentication and accounting statistics:

```
host1#show radius statistics
   RADIUS Authentication Statistics
   --------------------------------
     Statistic        10.10.121.128
-------------------   -------------
UDP Port              1812
Round Trip Time       0
Access Requests       0
```

```
Rollover Requests     0
Retransmissions       0
Access Accepts        0
Access Rejects        0
Access Challenges     0
Malformed Responses   0
Bad Authenticators    0
Requests Pending      0
Request Timeouts      0
Unknown Responses     0
Packets Dropped       0

     RADIUS Accounting Statistics
     ----------------------------
     Statistic        10.10.121.128
------------------   -------------
UDP Port              1646
Round Trip Time       2
Requests              1
Start Requests        1
Interim Requests      0
Stop Requests         0
Reject Requests       0
Rollover Requests     0
Retransmissions       3
Responses             1
Start Responses       1
Interim Responses     0
Stop Responses        0
Reject Responses      0
Malformed Responses   0
Bad Authenticators    0
Requests Pending      0
Request Timeouts      3
Unknown Responses     0
Packets Dropped       0
```

To display RADIUS pre-authentication statistics:

```
host1#show radius pre-authentication statistics

 RADIUS Pre-Authentication Statistics
 ------------------------------------
     Statistic        172.28.30.117
------------------   -------------
UDP Port              1812
Round Trip Time       0
Access Requests       2809
Rollover Requests     0
Retransmissions       56
Access Accepts        2809
Access Rejects        0
Access Challenges     0
Malformed Responses   0
Bad Authenticators    0
Requests Pending      0
Request Timeouts      72
Unknown Responses     0
Packets Dropped       2
```


To display RADIUS route-download statistics:

```
host1#show radius route-download statistics

 RADIUS Route-Download Statistics
 --------------------------------
     Statistic        192.168.30.16
-------------------   -------------
UDP Port              1812
Round Trip Time       0
Access Requests       1613
Rollover Requests     0
Retransmissions       6
Access Accepts        1612
Access Rejects        1
Access Challenges     0
Malformed Responses   0
Bad Authenticators    0
Requests Pending      0
Request Timeouts      6
Unknown Responses     0
Packets Dropped       5
```

Meaning Table 35 on page 271 lists the **show radius statistics** command output fields.

NOTE: All descriptions apply to the primary, secondary, and tertiary RADIUS authentication and accounting servers.

Table 35: show radius statistics Output Fields

Field Name	Field Description
UDP Port	Number of the UDP port of a RADIUS server
Round Trip Time	Hundreds of seconds from request to response
Access Requests	Number of access requests sent to server
Rollover Requests	Number of requests coming into server as a result of the previous server timing out
Retransmissions	Number of retransmissions
Access Accepts	Number of Access-Accepts received from the server
Access Rejects	Number of Access-Rejects received from the server
Access Challenges	Number of access challenges received from the server
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)

Table 35: show radius statistics Output Fields *(continued)*

Field Name	Field Description
Bad Authenticators	Number of responses in which the authenticator is incorrect for the matching request. This can occur if the RADIUS secret for the client and server does not match.
Requests Pending	Number of requests waiting for a response
Request Timeouts	Number of requests that timed out
Unknown Responses	Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.
Packets Dropped	Number of packets dropped either because they are too short or the E Series router receives a response for which there is no corresponding request. For example, if the router sends a request and the request times out, the router removes the request from the list and sends a new request. If the server is slow and sends a response to the first request after the router removes the request, the packet is dropped.
Requests	Total number of accounting requests sent, which is the combined total of Start Requests, Interim Requests, Stop Requests, and Reject Requests
Start Requests	Number of accounting start requests sent; includes Acct-On, Acct-Start, Acct-Link-State, and Acct-Tunnel-Start requests
Interim Requests	Number of interim accounting requests
Stop Requests	Number of accounting stop requests sent; includes Acct-Off, Acct-Stop, Acct-Link-Stop, and Acct-Tunnel-Stop requests
Reject Requests	Number of accounting reject requests sent; includes Acct-Link-Reject and Acct-Tunnel-Reject requests
Responses	Number of accounting responses received from the server
Start Responses	Number of accounting start responses received; includes Acct-On, Acct-Start, Acct-Link-Start, and Acct-Tunnel-Start responses
Interim Responses	Number of interim accounting responses
Stop Responses	Number of accounting stop responses received; includes Acct-Off, Acct-Stop, Acct-Link-Stop, and Acct-Tunnel-Stop responses

Table 35: show radius statistics Output Fields *(continued)*

Field Name	Field Description
Reject Responses	Number of accounting reject responses received; includes Acct-Link-Reject and Acct-Tunnel-Reject responses

Related Documentation
- show radius statistics on page 337

Monitoring RADIUS SNMP Traps

Purpose Display the configuration of RADIUS SNMP traps.

Action To display RADIUS SNMP traps configuration information:

```
host1#show radius trap
trap for auth-server-not-responding enabled
trap for no-auth-server-responding disabled
trap for auth-server-responding enabled
trap for acct-server-not-responding enabled
trap for no-acct-server-responding disabled
trap for acct-server-responding disabled
```

Meaning A list of the configured RADIUS-related SNMP traps is displayed.

Related Documentation
- show radius trap

Monitoring RADIUS UDP Checksums

Purpose Display information about UDP checksums.

Action To display the status of RADIUS UDP checksums:

```
host1#show radius udp-checksum
enabled
```

Meaning RADIUS checksums status is either enabled or disabled.

Related Documentation
- show radius udp-checksum

Monitoring RADIUS Server IP Addresses

Purpose Display the IP address of the RADIUS servers.

Action To display the RADIUS server IP address:

```
host1#show radius update-source-address
192.168.1.228
```

Related Documentation

- show radius update-source-addr

CHAPTER 36

Verifying Active Subscriber Session Details

Monitoring Subscriber Information

Purpose Display active subscribers on the router. If you specify a username, the router displays only the users that match the username. When you issue the **show subscribers** command in the default VR, all users are displayed. When you issue the **show subscribers** command in a nondefault VR, only those users attached to that VR are displayed. The following list describes keywords that you can issue with the **show subscribers** command:

- You can specify the **domain**, **interface**, **port**, **profile**, **slot**, **username**, or **virtual-router** keyword on all routers to filter the results. If you do not specify a keyword, all active users are displayed.
- When you use the **interface** keyword to display detailed subscriber information by interface, you must also specify the **atm**, **ethernet**, or **lag** keyword, an interface specifier, and, optionally, a subinterface specifier.
- If you specify the **lag** keyword, the output displays active subscribers for the specified LAG interface. By default, the **aaa intf-desc-format include sub-intf enable** command includes the subinterface and S-VLAN ID in the LAG interface ID. Use the **aaa intf-desc-format include sub-intf disable** command to exclude the subinterface and S-VLAN ID from the LAG interface ID.
- The output displayed in the Interface field depends on the configuration of two commands at the time the subscriber logs in: **aaa intf-desc-format include sub-intf** and **aaa intf-desc-format include adapter** (for the E120 and E320 Broadband Services routers).
  - When you issue the **aaa intf-desc-format include sub-intf disable** command, the subinterface is stripped from the subscriber's interface field at login and is not displayed in the output. In the default state, or when you issue the **aaa intf-desc-format include sub-intf enable** command, the subinterface is included in the subscriber's interface field at login and is displayed in the output.
  - When you issue the **aaa intf-desc-format include adapter disable** command, the adapter is stripped from the subscriber's interface field at login and is not displayed in the output. In the default state, or when you issue the **aaa intf-desc-format include adapter enable** command, the adapter is included in the subscriber's interface field at login and is displayed in the output.

- Even when the subinterface has been stripped from the subscriber's interface field, you can still include the subinterface specifier in the **show subscribers interface** command. Even though the subinterface itself is not displayed, only subscribers on the specified subinterface are displayed.
- The above considerations do not apply when you issue the **summary** keyword. The output displayed in the Interface field of summary versions is not affected by the state of either the **aaa intf-desc-format include sub-intf** command or the **aaa intf-desc-format include adapter** command when the subscriber logs in.

- You can issue the **ipv6** keyword to display all IPv6 subscribers or include the IPv6 prefix to limit the display to only IPv6 subscribers on a specific network.
- You can issue the **icr-partition** keyword to display active subscribers for a particular ICR partition configured on a chassis.

NOTE: If you attempt to bring up tunneled subscribers on ACI-based VLAN subinterfaces on LAC devices with subscriber groups that are based on S-VLAN IDs (using the **ip vrrp** *vrid* **icr-partition group svlan** command on S-VLAN subinterfaces), the VLAN subinterface does not come up and a log message to denote its down state is not generated. If you attempt to bring up tunneled subscribers on ACI-based VLAN subinterfaces on LAC devices with subscriber groups that are based on VLAN IDs (using the **ip vrrp** *vrid* **icr-partition group vlan** command on VLAN subinterfaces), the subscribers over tunnels are brought up. However, on the LAC device, the subscribers are logged in outside of the ICR partition.

This behavior is expected when attempts are made to log in tunneled subscribers over ACI-based VLAN subinterfaces configured with ICR partitions with VLAN-based grouping or S-VLAN-based grouping.

- You can use the **profile** keyword to list subscribers who share the same profile.
- You can specify the **summary** keyword to display only summary information about active subscribers.
- In the Interface field in the output of the **show subscribers** command, for subscribers that are logged in to the router over VLAN interfaces configured on the LAG bundle using protocols such as DHCP or PPPoE, the logged-in subscriber name is displayed against the LAG bundle on the member interface where the user session is established. The subscriber sessions are displayed for the corresponding major interfaces, such as Ethernet, only if the subscribers are logged in over VLAN subinterfaces configured over major interfaces.

Action To display general subscriber information:

```
host1# show subscribers

                                Subscriber List
                                ---------------
                                                                Virtual
```

```
      User Name           Type         Addr|Endpt           Router
----------------------   -----   --------------------   ------------
fred                     tst     10.10.65.86/radius     default
bert                     tst     192.168.10.3/user      default
      User Name                     Interface
----------------------   --------------------------------
fred                     atm 2/1.42:100.104
bert                     FastEthernet 5/2.4
      User Name              Login Time           Circuit Id
----------------------   -------------------   ----------------
fred                     06/05/12 10:58:42     atm 5/1.3
bert                     06/05/12 10:59:08
     User Name              Remote Id
----------------------   ----------------
fred
bert                     (800) 555-1212
```

To display detailed information about subscribers on the specified interface:

```
host1# show subscribers interface ethernet 5/2
                                Subscriber List
                                ---------------
                                                                  Virtual
       User Name           Type         Addr|Endpt             Router
------------------------   -----   --------------------   ------------
bert                       tst     192.168.10.3/user      default
       User Name                     Interface
------------------------   --------------------------------
bert                       FastEthernet 5/2.4
       User Name              Login Time           Circuit Id
------------------------   -------------------   ----------------
bert                       06/05/12 10:59:08
       User Name              Remote Id
-----------------------    ----------------
bert                       (800) 555-0000
```

To display detailed information about subscribers on the specified LAG interface:

```
host1# show subscribers interface lag lag2.1:1-1

                          Subscriber List
                          ---------------

User Name               Type      Addr|Endpt      Router
-------------            -----     -----------    ---------
4101DHCPCLIENT@CT.NET     ip     2.0.0.3/user    default

User Name                  Interface
------------------------  ------------
4101DHCPCLIENT@CT.NET     lag lag2.1:1-1

User Name                  Login Time            Circuit Id
------------------------  -------------------     ----------------
4101DHCPCLIENT@CT.NET     09/10/29 02:07:51

User Name                  Remote Id
------------------------   ----------------
4101DHCPCLIENT@CT.NET
```

To display detailed information about subscribers on the specified slot:

```
host1# show subscribers slot 5
                            Subscriber List
                            ---------------
                                                                  Virtual
       User Name            Type         Addr|Endpt              Router
------------------------   -----   --------------------   ------------
fred                       tst     10.10.65.86/radius     default
       User Name                       Interface
------------------------   --------------------------------
fred                       atm 5/1.42:100.104
       User Name               Login Time           Circuit Id
------------------------   -------------------   ----------------
fred                       06/05/12 10:58:42     atm 5/1.3
       User Name               Remote Id
-----------------------    ----------------
fred
```

To display detailed information about subscribers who share the same profile:

```
host1# show subscribers profile aaa
                            Subscriber List
                            ---------------
                                                                  Virtual
       User Name            Type         Addr|Endpt              Router
------------------------   -----   --------------------   ------------
user                       ppp     20.10.10.3/local       default
user                       ppp     20.10.10.8/local       default
       User Name                       Interface
------------------------   --------------------------------
user                       FastEthernet 1/5
user                       FastEthernet 1/5
       User Name               Login Time           Circuit Id
------------------------   -------------------   ----------------
user                       12/08/21 11:36:05
user                       12/08/22 16:34:53
       User Name               Remote Id              Profile Name
------------------------   ----------------   ------------------------
user                                          aaa
user                                          aaa
```

To display the number of subscribers who share the same profile:

```
host1# show subscribers summary profile

          Profile Name             Count
-------------------------------   ------
aa                                2
aaa                               2
aab                               2
Total Subscribers : 6 (chassis-wide total)
Peak  Subscribers : 6 (chassis-wide total)
```

To display the number of subscribers on each virtual router, as well as the total and peak subscribers for the chassis:

```
host1#show subscribers summary
  Virtual
   Router      Subscribers     Ppp       Ip      Tnl     Total
------------   ------------   ------   ------   ------   ------
default        1              1        0        0        1
```

```
Total Subscribers : 10 (chassis-wide total)
Peak  Subscribers : 15 (chassis-wide total)
```

To display the number of subscribers on each port:

```
host1#show subscribers summary port
Interface      Count
------------   ------
3/1            5
2/1            5
Total Subscribers : 10 (chassis-wide total)
Peak  Subscribers : 15 (chassis-wide total)
```

To display the number of subscribers by domain name:

```
host1#show subscribers summary domain
          Domain Name              Count
-------------------------------   ------
abc.com                           5
iii.com                           5
Total Subscribers : 10 (chassis-wide total)
Peak  Subscribers : 15 (chassis-wide total)
```

To display the number of subscribers by interface:

```
host1#show subscribers summary interface

Interface                Count
--------------------     -----
ATM 3/2.1                  1
ETHERNET 5/2.1              2
LAG lag1.100                1
Total Subscribers: 4 (chassis-wide total)
Peak Subscribers:  8 (chassis-wide total)
```

To display the number of subscribers by slot:

```
host1#show subscribers summary slot
  Slot     Count
--------   -----
3          1
5          4
Total Subscribers : 5 (chassis-wide total)
Peak  Subscribers : 8 (chassis-wide total)
```

To display the number of subscribers by ICR partition:

```
host1#show subscribers summary icr-partition
         ICR-Partition (location-id)              Count
-----------------------------------------      --------
3/0.1.4                                        5
3/0.2.5                                        5
Total Subscribers: 10 (chassis-wide total)
Peak Subscribers: 15 (chassis-wide total)
```

To display the number of subscribers that are logged in on top of a LAG bundle:

```
host1#show subscribers summary lag
     Interface         Count
--------------------   ------
LAG OLT                6
```

```
Total Subscribers : 6 (chassis-wide total)
Peak  Subscribers : 6 (chassis-wide total)
```

Meaning Table 36 on page 280 lists the **show subscribers** command output fields.

Table 36: show subscribers Output Fields

Field Name	Field Description
User Name	Name of the subscriber
Type	Type of subscriber: atm, ip, ipsec, ppp, tnl (tunnel), or tst (test)
Addr | Endpt	IP or IPv6 address and source of the address: l2tp, local, dhcp, radius, or user. For local, dhcp, radius, and user endpoints, the address is that of the user. When the endpoint is l2tp, the address is that of the LNS.
Virtual Router	Name of the virtual router context
Interface	Interface specifier over which the subscriber is connected
Login Time	Date, in YY/MM/DD format, and time the subscriber logged in
Circuit Id	User circuit ID value specified by PPPoE
Remote Id	User remote ID value specified by PPPoE
Total Subscribers	Number of active subscribers, chassis-wide
Peak Subscribers	Maximum value that is displayed in the Total Subscriber field during the time the router has been active, chassis-wide
Subscribers	Number of subscribers; the sum of the Ppp and Ip fields
Ppp	Number of PPPoA and PPPoE users, combined
Ip	Number of DHCP and IP subscriber manager users, combined
Tnl	Number of users tunneled to an LNS
Total	Total number of users per virtual router; the sum of the Ppp, Ip, and Tnl fields
Domain Name	Domain name used by the subscriber

Table 36: show subscribers Output Fields *(continued)*

Field Name	Field Description
ICR-Partition (location-id)	A unique identifier for each ICR partition on a chassis. Note that this ID is different from the partition name, which is configured using the **ip vrrp vrid icr-partition** *partitionName* command.
Count	Number of subscribers
Slot	Number of slot in the chassis

Related Documentation

- show subscribers on page 343

CHAPTER 37

Investigating Causes for Termination of User Sessions

Monitoring Application Terminate Reason Mappings

Purpose Display information about the mappings for application terminate reasons.

Action To display the current terminate reasons that are mapped to a specific Acct-Terminate-Cause-Code:

This example uses the **radius** keyword to display all current terminate reasons mapped to RADIUS Acct-Terminate-Cause codes. The output lists all PPP mappings, followed by L2TP mappings, and then AAA mappings.

```
host1(config)#run show terminate-code radius
                                                                    Radius
  Apps          Terminate Reason              Description           Code
---------   --------------------------   --------------------------   ------
ppp         authenticate-authenticator   authenticate authenticator     17
            -timeout                      timeout
ppp         authenticate-challenge-tim   authenticate challenge tim     10
            eout                         eout
ppp         authenticate-chap-no-resou   authenticate chap no resou     10
            rces                         rces
ppp         authenticate-chap-peer-aut   authenticate chap peer aut     17
            henticator-timeout           henticator timeout
ppp         authenticate-deny-by-peer    authenticate deny by peer      17
ppp         authenticate-inactivity-ti   authenticate inactivity ti     4
            meout                        meout
ppp         authenticate-max-requests    authenticate max requests      10
 --More--
```

To display all terminate reasons that are mapped to a specific terminate code:

This example uses the **radius** keyword and a RADIUS Acct-Terminate-Cause code (**radius 4**) to display all terminate reasons mapped to the specified terminate code.

```
host1(config)#run show terminate-code radius 4
                                                                    Radius
  Apps          Terminate Reason              Description           Code
---------   --------------------------   --------------------------   ------
ppp         authenticate-inactivity-ti   authenticate inactivity ti     4
```

```
           meout                          meout
l2tp       session-timeout-inactivity     session timeout inactivity     4
```

To display all current mappings for a particular application's terminate reasons:

This example uses **aaa** as the application.

```
host1(config)#run show terminate-code aaa
                                                                        Radius
  Apps          Terminate Reason              Description               Code
---------   --------------------------   --------------------------   ------
aaa         deny-server-not-available    deny server not available      17
aaa         deny-server-request-timeou   deny server request timed      17
            t                            out
aaa         deny-authentication-failur   deny authentication failur     17
            e                            e from server
aaa         deny-address-assignment-fa   deny address assignment fa     17
            ilure                        ilure
aaa         deny-address-allocation-fa   deny address allocation fa     17
            ilure                        ilure
aaa         deny-no-address-allocation   deny insufficient resource     17
            -resources                   s for address allocation
aaa         deny-unknown-subscriber      deny no such server entry      17
aaa         deny-no-resources            deny no resources availabl     10
                                         e
 --More--
```

To display the mapping for a specific terminate reason for an application:

This example uses **l2tp** as the application and **session-access-interface-down** as the terminate reason.

```
host1#show terminate-code l2tp session-access-interface-down
                                                                  Radius
                Terminate Reason Description                       Code
-----------------------------------------------------------------  ------
session access interface down                                       8
```

Meaning Table 37 on page 284 lists the **show terminate-code** command output fields.

Table 37: show terminate-code Output Fields

Field Name	Field Description
Apps	The application generating the terminate reason; AAA, L2TP, PPP, or RADIUS client
Terminate Reason	The application's terminate reason
Description	The terminate reason
Radius Code	The RADIUS Acct-Terminate-Cause code to which the application's terminate reason is mapped

Related Documentation

- show terminate-code

CHAPTER 38

Monitoring IPv6 Local Address Pool Settings

Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements for all Configured Pools

Purpose Display a summary of all the IPv6 local address pools configured on a virtual router, along with the prefix ranges in each of those pools, total number of prefixes that can be allocated to clients, and the number of prefixes that are in use by clients for Neighbor Discovery router advertisements.

Action To display information about all the IPv6 local address pools configured on a virtual router for Neighbor Discovery router advertisements:

```
host1#show ipv6 local ndra-pool
                              IPv6 Local Address ND-RA Pools
                              ------------------------
      Pool                  Start                       End                Total    In Use
----------------   -------------------------   -------------------------   -------   -------
ipv6Pool-expm1     2002:2002::/64              2002:2002:ffff::/64         65536     0
ipv6Pool-expm2     3003:3003::/48              3003:3003:ffff::/48         65536     0
example            4004:4004:0:ff00::/64       4004:4004:ffff::/48         65536     16000
```

Meaning Table 38 on page 286 lists the **show ipv6 local ndra-pool** command output fields.

Table 38: show ipv6 local ndra-pool Output Fields

Field Name	Field Description
Pool	Names of IPv6 Neighbor Discovery router advertisement local address pools configured on the virtual router
Start	Starting prefix of the range of prefixes configured in a particular Neighbor Discovery router advertisements pool
End	Ending prefix of the range of prefixes configured in a particular Neighbor Discovery router advertisements pool
Total	Number of prefixes available for allocation to clients from a particular Neighbor Discovery router advertisements pool
In Use	Number of prefixes in a pool that are currently used by Neighbor Discovery clients

Related Documentation

- IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview on page 46
- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements by Pool Name on page 286
- Monitoring IPv6 Local Pool Statistics for Neighbor Discovery Router Advertisements Allocation of Prefixes on page 287
- **show ipv6 local ndra-pool on page 331**

Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements by Pool Name

Purpose Display information about an IPv6 local address pool for Neighbor Discovery router advertisements configured on a virtual router.

Action To display information about an IPv6 local address pool for Neighbor Discovery router advertisements configured on a virtual router:

```
host1#show ipv6 local ndra-pool example

Pool : example
--------------
Utilization : 24

        Start               End                  Total   In Use   Exclude   Util
---------------         -------------------      ------  -------  -------   ----
2002:2002::/64           2002:2002:ffff::/64     65536   0        0         0
3003:3003::/64           3003:3003:0:1000::/64   17      0        0         0
```

```
4004:4004:0:ff00::/64     4004:4004:0:ffff::/64  256      0          0          0
```

Meaning Table 39 on page 287 lists the **show ipv6 local ndra-pool *poolName*** command output fields.

Table 39: show ipv6 local ndra-pool poolName Output Fields

Field Name	Field Description
Pool	Names of IPv6 Neighbor Discovery router advertisements local address pools configured on the virtual router
Start	Starting prefix of the range of prefixes configured in a particular Neighbor Discovery router advertisements pool
End	Ending prefix of the range of prefixes configured in a particular Neighbor Discovery router advertisements pool
Total	Number of prefixes available for allocation to clients from a particular Neighbor Discovery router advertisements pool
In Use	Number of prefixes in a pool that are currently used by Neighbor Discovery clients
Exclude	Prefix length or prefix range excluded
Util	Percentage of prefixes currently allocated to clients from a particular prefix range in the Neighbor Discovery router advertisements pool

Related Documentation

- IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview on page 46
- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements for all Configured Pools on page 285
- Monitoring IPv6 Local Pool Statistics for Neighbor Discovery Router Advertisements Allocation of Prefixes on page 287
- **show ipv6 local ndra-pool on page 331**

Monitoring IPv6 Local Pool Statistics for Neighbor Discovery Router Advertisements Allocation of Prefixes

Purpose Display IPv6 local address pool statistics used for Neighbor Discovery router advertisements to requesting routers.

Action To display all IPv6 local address pool statistics for Neighbor Discovery router advertisements to requesting routers:

```
host1#show ipv6 local ndra-pool statistics
IPv6 Local Address Pool Statistics
----------------------------------
    Statistic       Value
----------------    -----
Allocations         0
Allocation Errors   0
Releases            0
Release Errors      0
```

Meaning Table 40 on page 288 lists the **show ipv6 local ndra-pool statistics** command output fields.

Table 40: show ipv6 local ndra-pool statistics Output Fields

Field Name	Field Description
Allocations	Number of prefixes allocated to Neighbor Discovery router advertisements clients from the local address pool
Allocation Errors	Number of errors encountered during the allocation of prefixes
Releases	Number of prefixes released back to the pool
Release Errors	Number of errors encountered during the process of release of previously assigned prefixes by the requesting router

Related Documentation

- IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview on page 46
- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements for all Configured Pools on page 285
- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements by Pool Name on page 286
- **show ipv6 local ndra-pool on page 331**

Monitoring IPv6 Local Pools for DHCP Prefix Delegation By All Configured Pools

Purpose Display a summary of all the IPv6 local address pools configured on a virtual router, along with the prefix ranges in each of those pools, total number of prefixes that can be allocated to clients, and the number of prefixes that are in use by clients.

Action To display information about all the IPv6 local address pools configured on a virtual router:

```
host1#show ipv6 local pool
                                IPv6 Local Address Pools
                                ------------------------
      Pool                  Start                       End                Total    In Use
----------------   -------------------------   -------------------------   -------   -------
ipv6Pool-pppoa     2002:2002::/48              2002:2002:ffff::/48         65536     0
ipv6Pool-pppoe     3003:3003::/48              3003:3003:ffff::/48         65536     0
example            4004:4004::/48              4004:4004:ffff::/48         65536     16000
```

Meaning Table 41 on page 289 lists the **show ipv6 local pool** command output fields.

Table 41: show ipv6 local pool Output Fields

Field Name	Field Description
Pool	Names of IPv6 local address pools configured on the virtual router
Start	Starting prefix of the range of prefixes configured in a particular pool
End	Ending prefix of the range of prefixes configured in a particular pool
Total	Number of prefixes available for allocation to clients from a particular pool
In Use	Number of prefixes in a pool that are currently used by DHCPv6 clients

Related Documentation

- show ipv6 local pool on page 330

Monitoring IPv6 Local Pools for DHCP Prefix Delegation By Pool Name

Purpose Display prefix delegation details for an IPv6 local address pool configured on a virtual router.

Action To display prefix delegation information for a specific IPv6 local address pool:

```
host1#show ipv6 local pool example

Pool : example
--------------
Utilization : 24

        Start           End                Total   In Use   Exclude   Util   Preferred     Valid
                                                                              Lifetime     Lifetime
---------------      -------------------   ------  -------  -------   ----   -----------  ----------
4004:4004::/48       4004:4004:ffff::/48   65536    16000   1         24     30 minutes    1 day

Exclude                4004:4004::/48
```

```
Dns Servers             5:5:5:5:5:5:5:5
                        6:6:6:6:6:6:6:6
Domain Search List      example-1.com
                        example-2.com
                        example-3.com
                        example-4.com
```

Meaning Table 42 on page 290 lists the **show ipv6 local pool** *poolName* command output fields.

Table 42: show ipv6 local pool poolName Output Fields

Field Name	Field Description
Pool	Name of the IPv6 local address pool for which prefix delegation details are displayed
Utilization	Percentage of IPv6 prefixes currently allocated to clients from the local address pool
Start	Starting prefix of the range of prefixes configured in a particular pool
End	Ending prefix of the range of prefixes configured in a particular pool
Total	Number of prefixes available for allocation to clients from a particular pool
In Use	Number of prefixes in a pool that are currently used by DHCPv6 clients
Preferred Lifetime	Amount of time for which the prefix remains preferred for the requesting router to use
Valid Lifetime	Amount of time for which the prefix remains valid for the requesting router to use
Exclude	Prefix length or prefix range excluded from allocation to the requesting router
Util	Percentage of prefixes currently allocated to clients from a particular prefix range in the pool
Dns Servers	List of IPv6 addresses of DNS servers to be sent to clients in the DHCPv6 responses
Domain Search List	List of domain names configured in the IPv6 local pool for DNS resolution

Related Documentation

- show ipv6 local pool on page 330

Monitoring IPv6 Local Pool Statistics for DHCP Prefix Delegation

Purpose Display IPv6 local address pool statistics used for DHCP prefix delegation to requesting routers.

Action To display all IPv6 local address pool statistics for prefix delegation to clients:

```
host1#show ipv6 local pool statistics
IPv6 Local Address Pool Statistics
----------------------------------
    Statistic       Value
----------------    -----
Allocations         0
Allocation Errors   0
Releases            0
Release Errors      0
```

Meaning Table 43 on page 291 lists the **show ipv6 local pool statistics** command output fields.

Table 43: show ipv6 local pool statistics Output Fields

Field Name	Field Description
Allocations	Number of prefixes allocated to DHCPv6 clients from the local address pool
Allocation Errors	Number of errors encountered during the allocation of prefixes
Releases	Number of prefixes released back to the pool
Release Errors	Number of errors encountered during the process of release of previously assigned prefixes by the requesting router

Related Documentation

- show ipv6 local pool on page 330

CHAPTER 39

Monitoring Commands

baseline aaa

Syntax baseline aaa

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a statistics baseline for authentication and authorization statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline aaa route-download

Syntax baseline aaa route-download [ipv6]

Release Information Command introduced in JunosE Release 8.1.0.
ipv6 keyword added in JunosE Release 13.0.0.

Description Sets a statistics baseline for route downloads. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options
- ipv6—Sets a baseline for IPv6 route downloads

Mode Privileged Exec

baseline cops

Syntax baseline cops

Release Information Command introduced in JunosE Release 7.1.0.

Description Sets a baseline for the Common Open Policy Service (COPS) statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline local pool

Syntax baseline local pool

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a statistics baseline for the router local address pool statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline radius

Syntax baseline radius

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a statistics baseline for RADIUS statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline sscc

Syntax baseline sscc

Release Information Command introduced in JunosE Release 7.1.0.

Description Sets a baseline for the SRC statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

show aaa accounting

Syntax show aaa accounting [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays AAA accounting configuration information, including the destinations where broadcast and duplicate accounting records are sent.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa accounting default

Syntax show aaa accounting { *subscriberType* } default [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the AAA accounting method used for the particular type of subscriber.

Options

- *subscriberType*—Specifies the type of subscriber:
  - atm1483—ATM 1483 subscribers
  - ip—IP subscriber management interfaces
  - ipsec—IPsec subscribers
  - ppp—PPP subscribers
  - radius-relay—RADIUS relay subscriber
  - tunnel—Tunnel subscribers
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa authentication default

Syntax show aaa authentication { *subscriberType* } default [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the AAA authentication method list used for the particular type of subscriber.

Options

- *subscriberType*—Specifies the type of subscriber:
  - atm1483—ATM 1483 subscribers
  - ip—IP subscriber management interfaces
  - ipsec—IPsec subscribers
  - ppp—PPP subscribers
  - radius-relay—RADIUS relay subscriber
  - tunnel—Tunnel subscribers
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa delimiters

Syntax show aaa delimiters [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the domain name and realm name delimiters, parse order, and parse direction configured on the router.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa strip-domain

Syntax show aaa strip-domain

Release Information Command introduced in JunosE Release 12.0.0.

Description Displays information about the aaa domain-name stripping functionality per virtual router.

Mode Privileged Exec

Related Documentation
- aaa strip-domain

show aaa domain-map

Syntax show aaa domain-map [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the mapping between user domains and virtual routers. The display includes a tunnel group if one is assigned to the domain map.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa duplicate-address-check

Syntax show aaa duplicate-address-check [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures AAA to query the routing table for duplicate address assignment before granting access.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa duplicate-prefix-check-extension

Syntax show aaa duplicate-prefix-check-extension [*filter*]

Release Information Command introduced in JunosE Release 12.2.0.

Description Displays whether enhanced duplicate IPv6 prefix checking is enabled or disabled.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa ipv6-nd-ra-prefix

Syntax show aaa ipv6-nd-ra-prefix [*filter*]

Release Information Command introduced in JunosE Release 10.1.0.

Description Displays the RADIUS attribute used for IPv6 Neighbor Discovery router advertisements.

Options
- *filter*—See Filtering show Commands.

Mode Privileged Exec

show aaa dhcpv6-delegated-prefix

Syntax show aaa dhcpv6-delegated-prefix [*filter*]

Release Information Command introduced in JunosE Release 10.1.0.

Description Displays the RADIUS attribute used for DHCPv6 Prefix Delegation.

Options
- *filter*—See Filtering show Commands.

Mode Privileged Exec

show aaa model

Syntax show aaa model [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays AAA model.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa name-servers

Syntax show aaa name-servers [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the IP addresses of the primary and secondary DNS and WINS name servers.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa profile

Syntax show aaa profile [brief | name *profileName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays AAA profile names and the actions associated with each specified AAA profile name.

Options
- brief—Displays the status and number of configured VCs for all ATM interfaces configured in the router
- *profileName*—Name of the profile you want to display
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa route-download

Syntax show aaa route-download [ipv6] [statistics [delta]] [*filter*]

Release Information Command introduced in JunosE Release 8.1.0.
ipv6 keyword added in JunosE Release 13.0.0.

Description Displays AAA route download statistics.

Options
- ipv6—Displays IPv6 route-download statistics
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa route-download routes

Syntax show aaa route-download routes [*vrfName*] [detail] [*filter*]

Release Information Command introduced in JunosE Release 8.1.0.

Description Displays information about AAA downloaded routes.

Options
- *vrfName*—Name of a virtual routing and forwarding instance to display
- detail—Displays detailed information about downloaded routes
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa route-download ipv6 routes

Syntax show aaa route-download ipv6 routes [*vrfName*] [detail] [*filter*]

Release Information Command introduced in JunosE Release 13.0.0.

Description Displays information about AAA-downloaded IPv6 routes.

Options
- *vrfName*—Name of the VRF
- detail—Displays detailed information about downloaded routes
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa route-download routes global

Syntax show aaa route-download routes global [start *startString*] [detail] [*filter*]

Release Information Command introduced in JunosE Release 8.1.0.

Description Displays information about AAA downloaded routes for all virtual routers and VRFs.

Options

- *startString*—String that specifies the first router context to display in the output; a maximum of 32 alphanumeric characters
- detail—Displays detailed information about the downloaded routes
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa route-download ipv6 routes global

Syntax show aaa route-download ipv6 routes global [start *startString*] [detail] [*filter*]

Release Information Command introduced in JunosE Release 13.0.0.

Description Displays information about AAA-downloaded IPv6 routes for all virtual routers and VRFs.

Options
- *startString*—String that specifies the first router context to display in the output; a maximum of 32 alphanumeric characters
- detail—Displays detailed information about the downloaded routes
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa statistics

Syntax show aaa statistics [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the authentication and authorization statistics.

Options
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa subscriber per-port-limit

Syntax show aaa subscriber per-port-limit [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the number of active subscribers on each interface.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa subscriber per-vr-limit

Syntax show aaa subscriber per-vr-limit [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the number of active subscribers on each virtual router.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa timeout

Syntax show aaa timeout [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the idle and session timeouts.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show aaa user accounting interval

Syntax show aaa user accounting interval [*filter*]

Release Information Command introduced in JunosE Release 9.0.0.

Description Displays the default accounting interval for users attached to this virtual router.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show cops info

Syntax show cops info [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about SRC (formerly SDX) sessions and about the COPS layer created for SRC sessions.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show cops statistics

Syntax show cops statistics [delta] [*filter*]

Release Information Command introduced in JunosE Release 7.1.0.

Description Displays statistics about SRC (formerly SDX) sessions.

Options
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show ip local alias

Syntax show ip local alias [*aliasName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the aliases for local address pools configured on your system.

Options
- *aliasName*—Name of a specific alias
- *filter*—See Filtering show Commands

Mode Privileged Exec

show ip local pool

Syntax show ip local pool [*poolName* | statistics [delta]] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the local address pools configured on the router.

Options
- *poolName*—Name of a specific local address pool
- statistics—Specifies that local pool statistics are to be shown
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec

show ip local shared-pool

Syntax show ip local shared-pool [*poolName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the shared local address pools configured on the router.

Options
- *poolName*—Name of a specific shared local address pool
- *filter*—See Filtering show Commands

Mode Privileged Exec

show ip route

Syntax show ip route [vrf *vrfName*] [*destination* [*ipMask*] [detail]] [all] [*protocol*] [*filter*]

To display summary information:

show ip route summary [vrf *vrfName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays current state of the routing table.

Options

- *vrfName*—Displays the contents of the IP routing table associated with a VRF
- *destination*—Specifies the IP address or domain name of the host to show
- *ipMask*—IP mask of the specific address to show
- detail—Displays detailed information about the specific prefix; currently shows the tag added by means of the **ip route** command
- all—Displays all routes in the routing table inserted from all protocols (not just the *best* routes that are used for forwarding)
- *protocol*—One of the following protocols for which you want to display the best routes in the routing table; no routes are displayed if routes for the specified protocol are not present in the routing table
  - access—Displays the best access-server routes (BGP) in the routing table
  - access-internal—Displays the best access-internal routes in the routing table
  - bgp—Displays the best BGP routes in the routing table
  - bgp-tunnel—Displays the best BGP tunnel routes in the routing table
  - dvmrp—Displays the best DVMRP routes in the routing table
  - isis—Displays the best IS-IS routes in the routing table
  - ldp—Displays the best LDP tunnel routes in the routing table
  - local—Displays the best locally connected routes in the routing table
  - mbgp—Displays the best MBGP routes in the routing table
  - ospf—Displays the best OSPF routes owned by in the routing table
  - other—Displays the best internal control routes in the routing table
  - rip—Displays the best RIP routes in the routing table
  - rsvp—Displays the best RSVP tunnel routes in the routing table

  - static—Displays the best static routes added by network management to the routing table
  - static-rpf—Displays the best static RPF routes added by network management to the routing table
- summary—Displays summary counters for all routes in the IP routing table
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show ipv6 local pool

Syntax show ipv6 local pool [*poolName* | statistics [delta]] [*filter*]

Release Information Command introduced in JunosE Release 10.1.0.

Description Displays information for all IPv6 local address pools configured on a virtual router, a particular IPv6 local address pool, or the IPv6 local address pool statistics for DHCPv6 prefix delegation.

Options

- *poolName*—Name of the IPv6 local address pool configured on the virtual router for which you want to view statistics, such as the number of clients to which prefixes have been allocated from this pool, starting and ending prefixes of the address range, and other prefix configuration parameters .
- statistics—Displays the IPv6 local address pool statistics details.
- delta—Displays statistics that have changed since the last baseline was set.
- *filter*—See Filtering show Commands.

Mode Privileged Exec, User Exec

show ipv6 local ndra-pool

Syntax show ipv6 local ndra-pool [*poolName* | statistics [delta]] [*filter*]

Release Information Command introduced in JunosE Release 13.0.0.

Description Displays information for all IPv6 local address pools configured on a virtual router, a particular IPv6 local address pool, or the IPv6 local address pool statistics for Neighbor Discovery router advertisements.

Options

- *poolName*—Name of the IPv6 local address pool configured on the virtual router that enables you to view prefix range, total number of prefixes that can be allocated, and the number of prefixes in use
- statistics—Displays IPv6 local address pool statistics details
- delta—Displays statistics that have changed since the last baseline was set
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

Related Documentation

- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements by Pool Name on page 286
- Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements for all Configured Pools on page 285
- Monitoring IPv6 Local Pool Statistics for Neighbor Discovery Router Advertisements Allocation of Prefixes on page 287

show license

Syntax show license [*licenseType*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
service-management keyword added in JunosE Release 7.2.0.

Description Displays all licenses or a specified license.

NOTE: The **show license l2tp-session** command remains in the CLI even though a separate L2TP license is no longer required to enable support for 32,000 L2TP sessions on supported systems.

Options
- *licenseType*—bfd, b-ras, ipsec-tunnels, ipv6, l2tp-session, nat, or service-management
- *filter*—See Filtering show Commands

Mode Privileged Exec

show radius algorithm

Syntax show radius algorithm [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the RADIUS algorithm that the RADIUS servers use.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show radius override

Syntax show radius override [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the current override settings configured on the RADIUS client (LNS) for the NAS-IP-Address [4], NAS-Port-Id [87], Calling-Station-Id [31], and NAS-Identifier [32] RADIUS attributes. The nas-info field in the command output indicates the virtual router that generates the NAS-IP-Address and NAS-Identifier attributes for AAA broadcast accounting packets.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show radius rollover-on-reject

Syntax show radius rollover-on-reject [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the configuration of the rollover-on-reject feature.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show radius servers

Syntax show radius [*serverType*] servers [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
pre-authentication keyword added in JunosE Release 8.1.0.

Description Displays information about the RADIUS servers configured on the router.

Options
- *serverType*—One of the following RADIUS server types:
  - authentication—Displays authentication information only
  - accounting—Displays accounting information only
  - dynamic-request—Displays dynamic-request information only
  - pre-authentication—Displays preauthentication information only
- *filter*—See Filtering show Commands

Mode Privileged Exec

Related Documentation
- Monitoring RADIUS Dynamic-Request Server Information

show radius statistics

Syntax show radius [*serverType*] statistics [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
pre-authentication keyword added in JunosE Release 8.1.0.

Description Displays statistics for the RADIUS servers configured on the router.

Options
- *serverType*—One of the following RADIUS server types:
  - authentication—Displays authentication statistics only
  - accounting—Displays accounting statistics only
  - dynamic-request—Displays dynamic-request statistics only
  - pre-authentication—Displays preauthentication statistics only
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec

Related Documentation
- Monitoring RADIUS Dynamic-Request Server Information

show radius tunnel-accounting

Syntax show radius tunnel-accounting [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about RADIUS accounting for L2TP tunnels.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec

show sscc info

Syntax show sscc info [brief] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about SRC (formerly SDX or SSC) servers and SRC client (formerly SSCC) statistics.

Options
- brief—Displays abbreviated SRC client and server information
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show sscc options

Syntax show sscc options

Release Information Command introduced in JunosE Release 10.2.0.

Description Displays information about SRC client options for the virtual router.

Mode Privileged Exec, User Exec

show sscc statistics

Syntax show sscc statistics [delta] [*filter*]

Release Information Command introduced in JunosE Release 7.1.0.

Description Displays statistics about SRC (formerly SDX or SSC) servers and SRC client (formerly SSCC) statistics.

Options
- delta—Displays baselined statistics
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show sscc version

Syntax show sscc version [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the SRC client (formerly SSCC) version number.

Options
- *filter*—See Filtering show Commands

Mode Privileged Exec, User Exec

show subscribers

Syntax

To display detailed information:

show subscribers [ipv6 [*ipv6Prefix*]]
[domain *domainName* | icr-partition *icrPartitionLocationId* |
interface { atm | ethernet | lag } *interfaceSpecifier* |
port *interfaceSpecifier* | profile *profileName* | slot *slotNumber* | username *userName* |
virtual-router *vrName*] [*filter*]

To display summary information:

show subscribers summary [domain | icr-partition | interface | port | profile | slot |
virtual-router | lag] [*filter*]

Release Information

Command introduced before JunosE Release 7.1.0.
interface, **atm**, and **ethernet** keywords added in JunosE Release 7.3.0.
slot keyword and *slotNumber* variable added in JunosE Release 7.3.0.
icr-partition keyword and *icrPartitionLocationId* variable added in JunosE Release 10.3.0.
lag keyword added to the **show subscribers** command in JunosE Release 11.0.0.
lag keyword added to the **show subscribers summary** command in JunosE Release 12.3.0.
profile keyword and *profileName* variable added in JunosE Release 13.3.0.

Description

Displays the active subscribers on your router.

Options

- ipv6—Displays IPv6 subscribers for the domain
- *ipv6Prefix*—Prefix that defines the IPv6 network that you want to filter
- *userName*—Username of the active subscriber
- domain—Displays active subscribers for the domain
- *domainName*—Domain name matching usernames of active subscribers
- icr-partition—Displays active subscribers for the ICR partition
- *icrPartitionLocationId*—Unique identifier for each ICR partition on a chassis. Note that this ID is different from the partition ID, which is configured using the **ip vrrp** *vrid* **icr-partition** *partitionId* command. The partition location ID that you specify here is a combination of the interface within the chassis on which the ICR partition is configured and the VRRP ID, which is system-defined and nonconfigurable.
- interface—Displays active subscribers for the specified interface: **atm**, **ethernet**, or **lag**. In the **summary** version, this command displays active subscribers for all ATM, Ethernet, and LAG interfaces.
- *interfaceSpecifier*—Particular interface. The format varies according to the interface type; see Interface Types and Specifiers.
- port—Displays active subscribers for the port
- profile—Displays subscribers based on profile name

- *profileName*—Displays subscribers that share the same profile name
- slot—Displays active subscribers for the slot
- *slotNumber*—Number of the chassis slot of the line module in the range 0–2 (ERX310 model), 0–6 (ERX7xx models), 0–13 (ERX14xx models), 0-5 (E120 router), and 0-16 (E320 router)
- virtual-router—Displays active subscribers for the VR
- *vrName*—Name of the VR to which interfaces of active subscribers are bound
- lag—Displays the consolidated information about active subscribers that are logged in on top of a LAG bundle
- *filter*—See Filtering show Commands
- summary—Displays the active subscribers for each domain, interface, port, slot, or virtual router

Mode Privileged Exec

PART 4

Troubleshooting

CHAPTER 40

SNMP Traps and System Logs for Authentication Failures

SNMP Traps and System Log Messages Overview

The router can send Simple Network Management Protocol (SNMP) traps to alert network managers when:

- A RADIUS server fails to respond to a request.
- A RADIUS server that previously failed to respond to a request (and was consequently removed from the list of active servers) returns to active service.

  Returning to active service means that the E Series RADIUS client receives a valid response to an outstanding RADIUS request after the server is marked unavailable.
- All RADIUS servers within a VR context fail to respond to a request.

The router also generates system log messages when RADIUS servers fail to respond or when they return to active service; no configuration is required for system log messages.

The following sections describe SNMP Traps and system log messages:

SNMP Traps

The router generates SNMP traps and system log messages as follows:

- If the first RADIUS server fails to respond to the RADIUS request, the E Series RADIUS client issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server timed out. The E Series RADIUS client will not issue another system log message or SNMP trap regarding this RADIUS server until the deadtime expires, if configured, or for 3 minutes if deadtime is not configured.
- The E Series RADIUS client then sends the RADIUS request to the second configured RADIUS server. If the second RADIUS server fails to respond to the RADIUS request,

the E Series RADIUS client again issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server timed out.

- This process continues until either the E Series RADIUS client receives a valid response from a RADIUS server or the list of configured RADIUS servers is exhausted. If the list of RADIUS servers is exhausted, the E Series RADIUS client issues a system log message and, if configured, an SNMP trap indicating that all RADIUS servers have timed out.

If the E Series RADIUS client receives a RADIUS response from a "dead" RADIUS server during the deadtime period, the RADIUS server is restored to active status.

If the router receives a valid RADIUS response to an outstanding RADIUS request, the E Series client issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server is now available.

System Log Messages

You do not need to configure system log messages. The router automatically sends them when individual servers do not respond to RADIUS requests and when all servers on a VR fail to respond to requests. The following are the formats of the warning level system log messages:

RADIUS [authentication | accounting] server *serverAddress* unavailable in VR *virtualRouterName* [; trying *next*ServerAddress]
RADIUS no [authentication | accounting] servers responding in VR *virtualRouterName*
RADIUS [authentication | accounting] server *serverAddress* available in VR *virtualRouterName*

Related Documentation

- Configuring SNMP Traps on page 349

CHAPTER 41

Configuring SNMP Traps

Configuring SNMP Traps

This section describes how to configure the router to send traps to SNMP when RADIUS servers fail to respond to messages, and how to configure SNMP to receive the traps.

To set up the router to send traps:

1. (Optional) Enable SNMP traps when a particular RADIUS authentication server fails to respond to Access-Request messages.

   host1(config)#radius trap auth-server-not-responding enable

2. (Optional) Enable SNMP traps when all of the configured RADIUS authentication servers on a VR fail to respond to Access-Request messages.

   host1(config)#radius trap no-auth-server-responding enable

3. (Optional) Enable SNMP traps when a RADIUS authentication server returns to active service.

   host1(config)#radius trap auth-server-responding enable

4. (Optional) Enable SNMP traps when a RADIUS accounting server fails to respond to a RADIUS accounting request.

   host1(config)#radius trap acct-server-not-responding enable

5. (Optional) Enable SNMP traps when all of the RADIUS accounting servers on a VR fail to respond to a RADIUS accounting request.

   host1(config)#radius trap no-acct-server-responding enable

6. (Optional) Enable SNMP traps when a RADIUS accounting server returns to active service.

   host1(config)#radius trap acct-server-responding enable

To set up SNMP to receive RADIUS traps:

1. Set up the appropriate SNMP community strings.

   host1(config)#snmp-server community admin view everything rw
   host1(config)#snmp-server community private view user rw

```
host1(config)#snmp-server community public view everything ro
```

2. Specify the interface whose IP address is the source address for SNMP traps.

```
host1(config)#snmp-server trap-source fastEthernet 0/0
```

3. Configure the host that should receive the SNMP traps.

```
host1(config)#snmp-server host 10.10.132.93 version 2c 3 udp-port 162 radius
```

4. Enable the SNMP router agent to receive and forward RADIUS traps.

```
host1(config)#snmp-server enable traps radius
```

5. Enable the SNMP on the router.

```
host1(config)#snmp-server
```

NOTE: For more information about these SNMP commands, see *JunosE System Basics Configuration Guide*.

Related Documentation

- radius trap acct-server-responding on page 171
- radius trap acct-server-not-responding on page 172
- radius trap no-acct-server-responding on page 173
- radius trap auth-server-responding on page 174
- radius trap auth-server-not-responding on page 175
- radius trap no-auth-server-responding on page 176
- snmp-server on page 178
- snmp-server community on page 179
- snmp-server enable traps on page 180
- snmp-server host on page 183
- snmp-server trap-source on page 186

CHAPTER 42

Troubleshooting RADIUS Preauthentication Failure

Troubleshooting Subscriber Preauthentication

Problem You can configure the router to send traps to SNMP when a RADIUS preauthentication server fails to respond to messages. To do so, you use the same procedure and commands as you do to configure SNMP traps for a RADIUS authentication server.

Solution For example, to enable SNMP traps when a particular RADIUS preauthentication server fails to respond to Access-Request messages, use the **radius trap auth-server-not-responding enable** command.

Related Documentation

- Configuring SNMP Traps on page 349
- radius trap auth-server-not-responding on page 175

PART 5

Index

Index

A

B

C

D

L

M

N

P

R

S

T

U

V

W