Chapter 1

Configuring Remote Access

This chapter describes how to configure remote access to an E-series router. This chapter discusses the following topics:

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.

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 *Chapter 3, Configuring RADIUS Attributes*.

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 *Managing DHCP* on page 391.

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.

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 ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

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)

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 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.

Before You Configure B-RAS

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

Configuration Tasks

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.

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.

license b-ras

- Use to specify the B-RAS license.
- The license is a unique string of up to 15 alphanumeric characters.

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

- You can purchase licenses that allow up to 2,000, 4,000, 8,000, 16,000, 32,000, or 48,000 simultaneous active IP, LAC, and bridged Ethernet interfaces.
- Example

  ```
  host1(config)#license b-ras jwmR4k8D
  ```

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

Mapping a User Domain Name 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.

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.

NOTE: If the default VR does not exist, authentication fails.

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.

aaa domain-map

- Use to map a user domain name to a virtual router or a loopback interface.
- When you specify only the domain name, the command sets the mode to Domain Map Configuration.
- Example

  host1(config)#**aaa domain-map juniper.net vrouter_1**
  host1(config)#**aaa domain-map none vrouter_all_purpose**
  host1(config)#**aaa domain-map default vrouter_all_purpose**
  host1(config)#**aaa domain-map 8005558934 vrouter_78**
  host1(config)#**aaa domain-map westford.com**
  host1(config-domain-map)#

- Use the **no** version to delete the map entry.

ip-hint

- Use to preallocate an IP address for the remote B-RAS user before authenticating the remote user.
- The address is passed as a *hint* in the authentication request.
- Example

  host1(config-domain-map)#**ip-hint enable**

- Use the **no** version to disable the feature.

ipv6-local-interface

- Use to map a user domain name to an IP version 6 (IPv6) loopback interface.
- The local interface identifies the interface information to use on the local (E-series) side of the subscriber's interface.
- Example

  host1(config)#**aaa domain-map westford.com**
  host1(config-domain-map)#**ipv6-local-interface 2001:db8::8000**

- Use the **no** version to delete the entry.

ipv6-router-name

- Use to map a user domain name to an IPv6 virtual router in Domain Map Configuration mode.
- Example

  host1(config)#**aaa domain-map westford.com**
  host1(config-domain-map)#**ipv6-router-name vroutv6**

- Use the **no** version to delete the entry.

local-interface

- Use to map a user domain name to a loopback interface.
- The local interface identifies the interface information to use on the local (E-series) side of the subscriber's interface.
- Example

  host1(config)#**aaa domain-map westford.com**
  host1(config-domain-map)#**local-interface 10.10.5.30**

- Use the **no** version to delete the entry.

router-name

- Use to map a user domain name to a virtual router.
- Example

  host1(config)#**aaa domain-map westford.com**
  host1(config-domain-map)#**router-name vrout**

- Use the **no** version to delete the entry.

Setting Up Domain Name and Realm Name Usage

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.

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.

aaa delimiter

- Use to configure delimiters for the domain and realm names. Specify one of the following keywords:
  - **domainName**—Configures domain name delimiters. The default domain name delimiter is @.
  - **realmName**—Configures realm name delimiters. The default realm name delimiter is NULL (no character). In this case, realm parsing is disabled (having no delimiter disables realm parsing).
- You can specify up to eight delimiters each for domain name and realm name.
- Example

  host1(config)#**aaa delimiter domainName @*/**

- Use the **no** version to return to the default.

aaa parse-direction

- Use to specify the direction the router uses to parse the username for the domain or realm name.
  - **domainName**—Specifies that the domain name is parsed. The router performs domain parsing from right to left by default.
  - **realmName**—Specifies that the realm name is parsed. The router performs realm parsing from left to right by default.
  - **left-to-right**—Router searches from the left-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.
  - **right-to-left**—Router searches from the right-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.
- Example

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

- Use the **no** version to return to the default: right-to-left parsing for domain names and left-to-right parsing for realm names.

aaa parse-order

- Use to specify which part of a username the router uses as the domain name. If a user's name contains both a realm name and a domain name, you can configure the router to use either name as the domain name.
  - **domain-first**—Router searches for a domain name first. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name. For example, if the username is usEast/lori@abc.com, the domain name is abc.com. If the router does not find a domain name, it then searches for a realm name if the realm delimiter is specified.
  - **realm-first**—Router searches for a realm name first. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. For example, if the username is usEast/lori@abc.com, the domain name is usEast. If no realm name is found, the router searches for a domain name.
- Example

  host1(config)#**aaa parse-order domain-first**

- Use the **no** version to return to the default, realm first.

strip-domain

- Use to strip the domain name from the username before sending an access-request message to the RADIUS server.
- By default, the domain name is the text after the last @ character. However, if you change the domain name parsing by using the **aaa delimiter**, **aaa parse-order**, or **parse-direction** command, the router strips the domain name and delimiter that result from the parsing.
- To stop stripping the username, use the **disable** keyword.
- Example

  host1(config)#**aaa domain-map xyz.com**
  host1(config-domain-map)#**strip-domain enable**

- Use the **no** version to return to the default, disabled.

Domain Name and Realm Name Examples

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 4 shows the username and domain name that result from the parsing action of the various commands.

Table 4: 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
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

Specifying a Single Name for Users from a Domain

Assigning a single username and a single password for all users associated with a domain provides better compatibility with some RADIUS servers. You can use this feature for domains that require the router to tunnel, but not terminate, PPP sessions.

When users request a PPP session, they specify usernames and passwords. During the negotiations for the PPP session, the router authenticates legitimate users.

NOTE: This feature works only for users authenticated by Password Authentication Protocol (PAP) and not by Challenge Handshake Authentication Protocol (CHAP).

If you configure this feature, the router substitutes the specified username and password for all authenticated usernames and passwords associated with that domain.

There are two options for this feature. The router can:

- Substitute the domain name for each username and one new password for each existing password.

  For example, if the domain name is xyz.com and you specify the password xyz_domain, the router associates the username xyz.com and the password xyz_domain with all users from xyz.com.

- Substitute one new username for each username and one new password for each existing password.

  For example, if the domain name is xyz.com and you specify the username xyz_group and the password xyz_domain, the router associates these identifiers with all users from xyz.com.

To use a single username and a single password for all users from a domain:

1. Access Domain Map Configuration mode using the **aaa domain-map** command.
2. Specify the new username and password using the **override-user** command.

aaa domain-map

- Use to map a domain name to a virtual router or to access Domain Map Configuration mode.
- Example

  host1(config)#**aaa domain-map xyz.com**
  host1(config-domain-map)#

- Use the **no** version to delete the map entry.

override-user

- Use to specify a single username and single password for all users from a domain in place of the values received from the remote client.
- Use only for domains that require the router to tunnel and not terminate PPP sessions.
- If you specify a password only, the router substitutes the domain name for the username and associates the new password with the user. If you specify a password only and you have configured the domain name *none* with the **aaa domain-map** command, the router rejects any users without domain names.
- If you specify a name and password, the router associates both the new name and password with the user.
- Example

  host1(config-domain-map)#**override-user name boston password abc**

- Use the **no** version to revert to the original username.

Configuring RADIUS Authentication and Accounting Servers

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.

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 5 lists the range of UDP ports the router uses for each type of RADIUS request.

Table 5: Local UDP Port Ranges by RADIUS Request Type

RADIUS Request Type	ERX-310, ERX-710, ERX-1410, and E120 Routers	ERX-1440 and E320 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 *Configuring Local Authentication Servers* on page 39 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 *Extensible Authentication Protocol* in *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol*.

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 continues to be sent to the authenticating virtual router, but not to 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.

Configuring AAA Duplicate Accounting

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

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

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
```

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)#
```

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.

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.

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**

aaa accounting broadcast

- Use to enable AAA broadcast accounting on a virtual router. Specifies that accounting records be sent to the accounting servers on the virtual routers in the named virtual router group.
- A virtual router group can be used in any virtual router context, not just the context in which it is created.
- Example

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

- Use the **no** version to disable the AAA broadcast accounting.

aaa accounting default

- Use to specify the accounting method used for a particular type of subscriber.
- Specify one of the following types of subscribers:
  - **atm1483**; this keyword is not supported
  - **tunnel**
  - **ppp**
  - **radius-relay**
  - **ipsec**
  - **ip** (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.

NOTE: Although the **atm1483** keyword is available in the CLI for this command, that subscriber type is not supported. The router does not support accounting for ATM 1483 subscribers.

- Specify one of the following types of accounting methods:
  - **radius**—RADIUS accounting for the specified subscribers.
  - **none**—No accounting is done for the specified subscribers.
  - **radius none**—Multiple types of accounting; used in the order specified. For example, **radius none** specifies that RADIUS accounting is initially used; however, if RADIUS servers are not available, no accounting is done.
- Example

  host1(config)#**aaa accounting ppp default radius**

- Use the **no** version to set the accounting protocol to the default, **radius**.

aaa accounting duplication

- Use to enable AAA duplicate accounting on a virtual router. Specifies that duplicate accounting records be sent to the accounting server on another virtual router.
- Example

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

- Use the **no** version to disable the feature.

aaa accounting immediate-update

- Use to send an accounting update to the accounting server immediately on receipt of a response for an Acct-Start message.
- Use the **enable** keyword to enable immediate updates. Use the **disable** keyword to disable immediate updates. Immediate updates are disabled by default.
- Example

  host1(config)#**aaa accounting immediate-update enable**

- Use the **no** version to restore the default condition, disabling immediate updates.

aaa accounting interval

- Use to specify the default interval between updates for user and service interim accounting.

NOTE: This command is deprecated and might be removed completely in a future release. Use the **aaa user accounting interval** command to specify the default interval for user accounting. Use the **aaa service accounting interval** command to specify the default interim accounting interval used for services created by the Service Manager application. See *Chapter 27, Configuring Service Manager*.

- Select an interval in the range 10–1440 minutes. The default is 0, which means that the feature is disabled.
- Example

  host1(config)#**aaa accounting interval 60**

- Use the **no** version to turn off interim accounting for both users and services.

aaa accounting statistics

- Use to specify how the AAA server collects statistics on the sessions it manages.
- Use the **volume-time** keyword to collect all statistics for the sessions.
- Use the **time** keyword to collect only the uptime status of the sessions. Collecting only uptime information is more efficient because less data is sent to AAA.
- Example

  host1(config)#**aaa accounting statistics time**

- Use the **no** version to restore the default, in which all statistics are collected.

aaa accounting vr-group

- Use to create an accounting virtual router group and enter VR Group Configuration mode. Virtual routing groups are used for AAA broadcast accounting.

- A virtual router group can have up to four virtual routers. The accounting servers of the virtual routers in the group receive broadcast accounting records that are forwarded to the group.
- The E-series router supports a maximum of 100 virtual router groups.
- When creating a virtual router group, you must add at least one virtual router to the group; otherwise, the group is not created.
- A virtual router group can be used in any virtual router context, not just the context in which it is created.
- Example

  host1(config)#**aaa accounting vr-group westVrGroup38**
  host1(config-vr-group)#

- Use the **no** version to delete the accounting virtual router group.

aaa authentication default

- Use to specify the authentication method used for a particular type of subscriber.
- Specify one of the following types of subscribers:
  - **atm1483**
  - **tunnel**
  - **ppp**
  - **radius-relay**
  - **ipsec**
  - **ip** (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.

- Specify one of the following types of accounting methods:
  - **radius**—RADIUS authentication for the specified subscribers.
  - **none**—Grants the specified subscribers access without authentication.
  - **radius none**—Multiple types of authentication; used in the order specified. For example, **radius none** specifies that RADIUS authentication is initially used; however, if RADIUS servers are not available, users are granted access without authentication.
- Example

  host1(config)#**aaa authentication ip default radius**

- Use the **no** version to set the authentication protocol to the default, **radius**.

aaa duplicate-address-check

- Use to enable or disable routing table address lookup or duplicate address check.

- The router checks the routing table for returned addresses for PPP users. If the address existed, then the user was denied access.
- You can disable this routing table address lookup or duplicate address check with the **aaa duplicate-address-check** command.
- Example

  host1(config)#**aaa duplicate-address-check enable**

- There is no **no** version.

aaa user accounting interval

- Use to specify the default interval between user accounting updates. The router uses the default interval when no value is specified in the RADIUS Acct-Interim-Interval attribute (RADIUS attribute 85).
- This command and the **aaa service accounting interval** command replace the **aaa accounting interva**l command, which is deprecated and might be removed in a future release. For information about setting the default interim accounting interval for services, see *Chapter 27, Configuring Service Manager*.
- The default interval is applied on a virtual router basis—this setting is used for all users who attach to the corresponding virtual router.
- Specify the user accounting interval in the range 10–1440 minutes. The default setting is 0, which disables the feature.
- Example

  host1(config)#**aaa user accounting interval 20**

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

aaa virtual-router

- Use to add virtual routers to a virtual router group. During AAA broadcast accounting, accounting records are sent to the accounting servers on the virtual routers in the named virtual router group.
- You can add up to four virtual routers to a virtual router group. Use the *indexInteger* parameter to specify the order (1–4) in which the virtual routers receive the accounting information. The *indexInteger* is used with the **no** version to delete a specific virtual router from a group (see Example 2).
- A virtual router name consists of 1–32 alphanumeric characters.
- The virtual router names in the group must be unique. An error message appears if you enter a duplicate name.
- Example 1

  host1(config)#**aaa accounting vr-group westVrGroup38**
  host1(config-vr-group)#**aaa virtual-router 1 vrWestA**
  host1(config-vr-group)#**aaa virtual-router 2 vrWestB**
  host1(config-vr-group)#**aaa virtual-router 4 vrSouth1**

- Example 2

  host1(config-vr-group)#**no aaa virtual-router 2**

- Use the **no** version of the command with the *indexInteger* parameter to delete a specific virtual router from a group. If all virtual routers in a group are deleted, the group is also deleted; a group must contain at least one virtual router.

deadtime

- Use to configure the amount of time (0–30 minutes) that a server is marked as unavailable if a request times out for the configured retry count.
- If a server fails to answer a request, the router marks it *unavailable*. The router does not send requests to the server until the router receives a response from the server or until the configured time is reached, whichever occurs first.
- If all servers fail to answer a request, then instead of marking all servers as unavailable, all servers are marked as available.
- To turn off the deadtime mechanism, specify a value of 0.
- Example

  host1(config)#**radius authentication server 10.10.0.1**
  host1(config-radius)#**deadtime 10**

- Use the **no** version to set the time to the default value, 0

key

- Use to configure secrets on the primary, secondary, and tertiary authentication servers.
- The authentication or accounting server secret is a text string used by RADIUS to encrypt the client and server *authenticator* field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string.
- The default is no server secret.
- Example

  host1(config)#**radius authentication server 10.10.8.1**
  host1(config-radius)#**key gismo**

- Use the **no** version to remove the secret.

NOTE: Authentication fails if no key is specified for the authentication server.

logout subscribers

- Use to issue an administrative reset to the user's connection to disconnect the user.
- From Privileged Exec mode, you can log out **all** subscribers, or log out subscribers by **username**, **domain**, **virtual-router**, or **port**.
- This command applies to PPP users, as well as to non-PPP DHCP users.

- Example

  host1#**logout subscribers username bmurphy**

- There is no **no** version.

max-sessions

- Use to configure the number of outstanding requests supported by an authentication or accounting server.
- If the request limit is reached, the router sends the request to the next server.

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 same IP address can be used for both an authentication and accounting server (but not for multiple servers of the same type). The router uses different UDP ports for authentication servers and accounting servers.
- For each multiple of 255 requests (the RADIUS protocol limit), the router opens a new UDP source (or local) port on the server to send and receive RADIUS requests and responses.
- Example

  host1(config)#**radius authentication server 10.10.0.1**
  host1(config-radius)#**max-sessions 100**

- Use the **no** version to restore the default value, 255.

no radius client

- Use to remove all RADIUS servers for the virtual router context and to delete the E-series RADIUS client for the virtual router context.
- Example

  host1:boston(config)#**no radius client**

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

radius algorithm

- Use to specify the algorithm—either **direct** or **round-robin**—that the E-series RADIUS client uses to contact the RADIUS server.
- Example

  host1(config)#**radius algorithm round-robin**

- Use the **no** version to set the algorithm to the default, **direct**.

radius override nas-info

- Use to configure the RADIUS client to include the NAS-IP-Address [4] and NAS-Identifier [32] RADIUS attributes of the authenticating virtual router in accounting packets when the client performs AAA broadcast accounting. Normally, the accounting packets include the NAS-IP-Address and NAS-Identifier of the virtual router that generated the accounting information.
- This override operation is a per-virtual router specification; use this command in the correct virtual router context.
- This command is ignored if the authenticating virtual router does not have a configured RADIUS server.
- Example

  host1(config)#**virtual-router vrXyz1**
  host1:vrXyz1(config)#**radius override nas-info**
  host1:vrXyz1(config)#**exit**

- Use the **no** version to restore inclusion of the NAS-IP-Address [4] and NAS-Identifier [32] RADIUS attributes of the virtual router that requested the accounting information.

radius rollover-on-reject

- Use to specify whether the router rolls over to the next RADIUS server when the router receives an Access-Reject message for the user it is authenticating.
- Example

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

- Use the **no** version to set the default of disable.

radius accounting server
radius authentication server

- Use to specify the IP address of **authentication** and **accounting** servers.
- Example

  host1(config)#**radius authentication server 10.10.10.1**
  host1(config-radius)**exit**
  host1(config)#**radius authentication server 10.10.10.2**
  host1(config-radius)**exit**
  host1(config)#**radius authentication server 10.10.10.3**
  host1(config-radius)**exit**
  host1(config)#**radius accounting server 10.10.10.20**
  host1(config-radius)**exit**
  host1(config)#**radius accounting server 10.10.10.30**

- Use the **no** version to delete the instance of the RADIUS server.

radius tunnel-accounting

- Use to specify that tunnel accounting be enabled or disabled.
- This command turns on accounting messages: Tunnel-Start, Tunnel-Stop, Tunnel-Reject, Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject, as described in RFC 2867.

- Your router supports tunnel accounting for the L2TP LAC and LNS.
- Example

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

- Use the **no** version to set the default, disabled.

radius udp-checksum

- Use to disable UDP checksums on virtual routers you configure for B-RAS.
- Issue this command in the context of the appropriate virtual router.
- Example

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

- Use the **no** version to reenable UDP checksums on virtual routers you configure for B-RAS.

radius update-source-addr

- Use to specify an alternate source IP address for the router to use rather than the default router ID.
- Example

  host1(config)#**radius update-source-addr 192.168.40.23**

- Use the **no** version to delete the parameter so that the router uses the router ID.

retransmit

- Use to set the maximum number of times that the router retransmits a RADIUS packet to an authentication or accounting server.
- If there is no response from the primary RADIUS authentication or accounting server in the specified number of retries, the client sends the request to the secondary server. If there is no response from the secondary server, the router sends the request to the tertiary server, and so on.
- Example

  host1(config)#**radius authentication server 10.10.8.1**
  host1(config-radius)#**retransmit 2**

- Use the **no** version to set the value to the default, 3 retransmits.

test aaa

- Use to verify RADIUS authentication and accounting and IP address assignment setup.
- You must specify either a PPP or Multilink PPP (MLPPP) user. PPP indicates a regular PPP user. MLPPP simulates Multilink PPP so that if multiple test commands are issued, all test users are bound by the same address.
- The command uses a username and password and attempts to authenticate a user, get an address assignment, and issue a start accounting request.

- Optionally, you can specify the virtual router context in which to authenticate the user.
- The command pauses for several seconds, then terminates the session by issuing a stop accounting request and an address release.
- Example

  host1#**test aaa ppp jsmith mypassword virtual-router charlie2**

NOTE: Specifying the password to associate with the username is optional. Specifying a virtual router is optional.

- There is no **no** version.

timeout

- Use to set the number of seconds before the router retransmits a RADIUS packet to an authentication or accounting server.
- If the interval is reached and there is no response from the primary RADIUS authentication or accounting server, the router attempts another retry. When the retry limit is reached, the client sends the request to the secondary server. When the retry limit for the secondary server is reached, the router attempts to reach the tertiary server, and so on.

NOTE: After the fourth retransmission, the configured timeout value is ignored, and the router uses a backoff algorithm that increases the timeout between each succeeding transmission.

The backoff algorithm is:

$$\text{timeout} = 2^{\text{retry-count}} + (\text{random}() \text{ modulo } 2^{\text{retry-count}})$$

g013623

- Example

  host1(config)#**radius authentication server 10.10.0.1**
  host1(config-radius)#**timeout 5**

- Use the **no** version to restore the default value, 3 seconds.

NOTE: When a RADIUS server times out or when it has no available RADIUS identifier values, the router removes the RADIUS server from the list of available servers for a period of time. The router restores all configured servers to the list if it is about to remove the last server. Restoring the servers avoids having an empty server list.

udp-port

- Use to configure the UDP port on the router where the RADIUS authentication, accounting, preauthentication, and route-download servers reside. The router uses this port to communicate with the RADIUS authentication servers.
- Specify a port number in the range 0–65536. For authentication, preauthentication, or route-download servers, the default UDP port is 1812. For accounting servers, the default is 1813.
- For an accounting server, specify a port number in the range 0–65536. The default is 1813.
- Example

  host1(config)#**radius authentication server 10.10.9.1**
  host1(config-radius)#**udp-port 1645**

- Use the **no** version to set the port number to the default value.

SNMP Traps and System Log Messages

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.

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*S*erverAddress*]

RADIUS no [authentication | accounting] servers responding in VR *virtualRouterName*

RADIUS [authentication | accounting] server *serverAddress* available in VR *virtualRouterName*

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 *Configuring Traps* in *JUNOSe System Basics Configuration Guide, Chapter 4, Configuring SNMP*.

radius trap acct-server-not-responding

- Use to enable or disable SNMP traps when a particular RADIUS accounting server fails to respond to a RADIUS accounting request.
- The associated SNMP object is rsRadiusClientTrapOnAcctServerUnavailable.

- Example

  host1(config)#**radius trap acct-server-not-responding enable**

- Use the **no** version to return to the default setting, disable.

radius trap acct-server-responding

- Use to enable or disable SNMP traps when a RADIUS accounting server returns to service after being marked as unavailable.
- The associated SNMP object is rsRadiusClientTrapOnAcctServerAvailable.
- This command affects only the current VR context.
- Example

  host1(config)#**radius trap acct-server-responding enable**

- Use the **no** version to restore the default, disable.

radius trap auth-server-not-responding

- Use to enable or disable SNMP traps when a RADIUS authentication server fails to respond to a RADIUS Access-Request message.
- The associated SNMP object is rsRadiusClientTrapOnAuthServerUnavailable.
- Example

  host1(config)#**radius trap auth-server-not-responding enable**

- Use the **no** version to return to the default setting, disabled.

radius trap auth-server-responding

- Use to enable RADIUS to send SNMP traps when a RADIUS authentication server returns to service after being marked as unavailable.
- The associated SNMP object is rsRadiusClientTrapOnAuthServerAvailable.
- This command affects only the current VR context.
- Example

  host1(config)#**radius trap auth-server-responding enable**

- Use the **no** version to restore the default setting, disabled.

radius trap no-acct-server-responding

- Use to enable or disable SNMP traps when all of the configured RADIUS accounting servers per VR fail to respond to a RADIUS accounting request.
- The associated SNMP object is rsRadiusClientTrapOnNoAcctServerAvailable.
- Example

  host1(config)#**radius trap no-acct-server-responding enable**

- Use the **no** version to return to the default setting, disabled.

radius trap no-auth-server-responding

- Use to enable or disable SNMP traps when all of the configured RADIUS authentication servers per VR fail to respond to a RADIUS Access-Request message.
- The associated SNMP object is rsRadiusClientTrapOnNoAuthServerAvailable.
- Example

  host1(config)#**radius trap no-auth-server-responding enable**

- Use the **no** version to return to the default setting, disabled.

Configuring Local Authentication Servers

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.

Creating the 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.

Creating 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**

Adding 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).

Using the username Command

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
```

Using the aaa local username Command

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**

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**

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
```

Configuration Commands

Use the following commands to configure the local authentication server.

aaa authentication default

- Use to specify that the local authentication method is used to authenticate PPP subscribers on the default virtual router or on the selected virtual router.

NOTE: You can specify multiple authentication methods; for example, **aaa authentication ppp default local radius**. If, during local authentication, the matching user entry is not found in a populated database or if it is found and rejected, the authentication procedure terminates. However, if the specified local user database is empty or if it does not exist, the authentication process uses the next authentication method specified (RADIUS in this case).

- Example

  ```
  host1(config)#aaa authentication ppp default local radius
  ```

- Use the **no** version to restore the default authentication method of **radius**.

aaa local database

- Use to create a local user database.
- Use the database name **default** to specify the default local user database, or enter a name for the specific local user database.
- Example

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

- Use the **no** version to delete the specified database and all entries in the database.

aaa local select database

- Use to assign the local user database that the virtual router uses for local authentication.
- Example

  host1(config)#**virtual-router cleveland**
  host1:cleveland(config)#**aaa local select database westLocal40**

- Use the **no** version to restore the default setting, which uses the default local user database for local authentication.

aaa local username

- Use to configure a user entry in the specified local user database and to enter Local User Configuration mode.
- The username must be unique within a particular database; however, the same username can be used in different databases.
- Use the database name **default** to configure the username in the default local user database.

NOTE: The router supports usernames up to 64 characters long; however, PAP and CHAP support is limited to 31-character usernames.

- Example

  host1(config)#**aaa local username cksmith database westLocal40**

- Use the **no** version to delete the user entry from the specified local user database. Use the database name **default** to delete the user entry from the default local user database.

ip-address

- Use to specify the IP address parameter for a user entry in the local user database. The address is negotiated with the subscriber after the subscriber is authenticated.
- Example

  host1(config-local-user)#**ip-address 192.168.42.6**

- Use the **no** version to delete the IP address parameter from the user entry in the local user database.

ip-address-pool

- Use to specify the IP address pool parameter for a user entry in the local user database. The address pool is used to assign an IP address to the subscriber; the address is negotiated with the subscriber after the subscriber is authenticated.
- Example

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

- Use the **no** version to delete the IP address pool parameter from the user entry in the local user database.

operational-virtual-router

- Use to specify the virtual router parameter for a user entry in the local user database. The subscriber is assigned to the operational virtual router only if the default virtual router performs the authentication.
- If authentication is performed by a non-default virtual router, then the subscriber is assigned to the same virtual router that performs authentication, regardless of this parameter setting.
- Example

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

- Use the **no** version to delete the operational virtual router parameter from the user entry in the local user database.

password

- Use to add a password to a user entry in the local user database. The password is used to authenticate a subscriber, and is encrypted by means of a two-way encryption algorithm.

NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- The new password replaces any current password or secret.
- Specify one of the following encryption algorithms, followed by the password:
  - 0—An unencrypted password; this is the default
  - 8—A two-way encrypted password
- Example

  host1(config-local-user)#**password 0 myPassword**

- Use the **no** version to delete the password or secret from the user entry in the local user database.

secret

- Use to add a secret to a user entry in the local user database. The secret is used to authenticate a subscriber, and is encrypted by means of the Message Digest 5 (MD5) encryption algorithm.

NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- The new secret replaces any current password or secret.
- Specify one of the following encryption algorithms, followed by the secret:
  - 0—An unencrypted secret; this is the default
  - 5—An MD5-encrypted secret
- Example

  host1(config-local-user)#**secret 5 Q3&t9REwk45jxSM#fj$z**

- Use the **no** version to delete the secret or password from the user entry in the local user database.

username

- Use to configure a user entry and optional password or secret in the default local user database. This command creates the database if it does not already exist.
- Optionally, specify a password or secret that is assigned to the user in the default local user database, or specify that no password is required for the particular username.
  - Specify one of the following encryption algorithms, followed by the password:
    - 0—An unencrypted password; this is the default
    - 8—A two-way encrypted password
  - Specify one of the following encryption algorithms, followed by the secret:
    - 0—An unencrypted secret; this is the default
    - 5—An MD5-encrypted secret
  - Use the **nopassword** keyword to remove the password or secret

NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- Example

  host1(config-local-user)#**username cksmith secret 5 Q3&t9REwk45jxSM#fj$z**

- Use the **no** version to delete the username entry from the default local user database.

Local Authentication Example

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 ERX-1400
! 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 ERX-1400
! 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 ERX-1400
! 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 ERX-1400
! 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 ERX-1400
! 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
```

Configuring Tunnel Subscriber Authentication

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 Topics

- **tunnel-subscriber authentication** command
- Mapping a User Domain Name to a Virtual Router on page 9

Configuring Name Server Addresses

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.

Configuration Tasks

This section contains procedures for configuring the DNS and WINS primary and secondary name server addresses.

DNS Primary and Secondary NMS Configuration

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.

aaa dns primary

- Use to specify the IP address of the DNS primary name server.
- Example

  host1(config)#**aaa dns primary 10.10.10.5**

- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa dns secondary

- Use to specify the IP address of the DNS secondary name server.
- Example

  host1(config)#**aaa dns secondary 10.10.10.6**

- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa ipv6-dns primary

- Use to specify the IPv6 address of the DNS primary name server.
- Example

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

- Use the **no** version to set the corresponding address to 0 (or ::).

aaa ipv6-dns secondary

- Use to specify the IPv6 address of the DNS secondary name server.
- Example

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

- Use the **no** version to set the corresponding address to 0 (or ::).

WINS Primary and Secondary NMS Configuration

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.

aaa wins primary

- Use to specify the IP address of the WINS primary name server.
- Example

  host1(config)#**aaa wins primary 192.168.10.05**

- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa wins secondary

- Use to specify the IP address of the WINS secondary name server.
- Example

  host1(config)#**aaa wins secondary 192.168.10.40**

- Use the **no** version to set the corresponding address to 0.0.0.0.

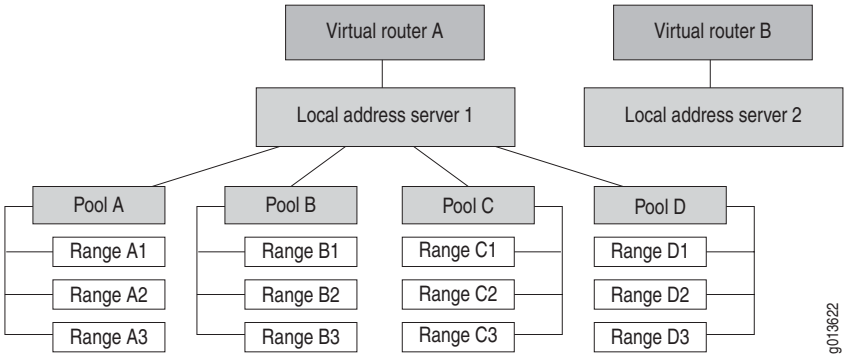
Configuring Local Address Servers

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 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



Local Address Pool Ranges

As shown in Figure 1, 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.

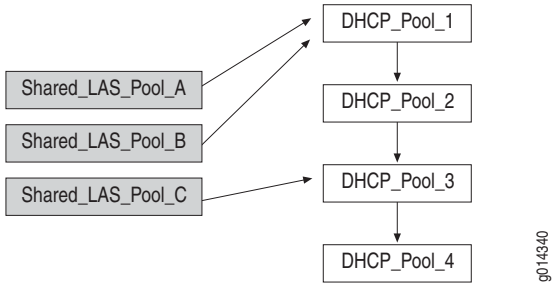
Shared Local Address Pools

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 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.

Example This following commands create the shared address pools in Figure 2 on page 54:

```
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

An 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 a pool's outstanding addresses 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 threshold utilization threshold, SNMP is notified.

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 an address pool name to a domain name.

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

- 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**

address-pool-name

- Use to specify the name of the local address pool from which the router allocates addresses for the domain that you are configuring.
- If the authentication server does not return an address, the router allocates an address from this pool. The authentication server may override this pool name using RADIUS attributes such as Framed-Pool.
- Example

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

- Use the **no** version to remove the address pool name.

ip address-pool

- Use to specify the addressing scheme: **dhcp**, **local**, or **none**.
- The addressing scheme **none** returns a special indicator to AAA that enables the remote PPP client to assign its own address.
- Example

  host1(config)#**ip address-pool dhcp**

- Use the **no** version to specify the default, local.

ip local alias

- Use to create an alias for an existing local address pool. The IP address is allocated from the pool specified by the alias rather than from the pool specified in the IP address request.
- An alias name may contain up to 16 characters.
- You can configure a maximum of 32 aliases per virtual router.
- A local address pool can have multiple aliases.
- You can set the name of the alias to match the name of a local address pool; however, the two names used in the alias cannot be the same.
- You can modify an existing alias with a different local address pool name.
- When a local address pool is deleted, all aliases with the matching pool name are also deleted.
- Example

  host1(config)#**ip local alias groupB pool-name addrpool_10**

- Use the **no** version to remove the alias name.

ip local pool

- Use to map an address pool name to a range of local addresses.
- You can create a pool with no address ranges configured for it.
- A name may contain up to 16 characters.
- Example

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

- Use the **no** version to remove the local pool (all ranges), or the specified range.

ip local pool snmpTrap

- Use to enable SNMP pool utilization traps.
- Example

  host 1(config)#**ip local pool addr_test snmpTrap**

- Use the **no** version to disable SNMP pool utilization traps.

ip local pool warning

- Use to set SNMP utilization warning threshold values.
- Example

  host1(config)#**ip local pool addr_test warning 90 80**

- Use the **no** version to reset the attributes to their default values; high threshold 85, abated threshold 75.

ip local shared-pool

- Use to create a local shared address pool and to specify the DHCP address pool that provides the addresses.
- You can reference a DHCP address pool that has not yet been configured.
- Example

  host1(config)#**ip local shared-pool sharedPool11 dhcpPool6**

- Use the **no** version to delete a specific local shared address pool.

Configuring 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

For more information about DHCP, see *Chapter 17, DHCP Overview*.

Creating an IP Interface

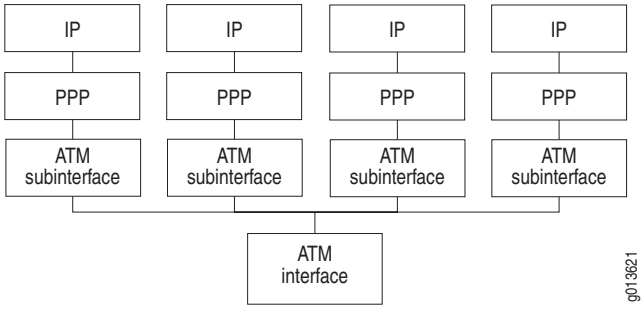
You can configure IP interfaces that support the following configurations:

- A single PPP client per ATM or Frame Relay subinterface
- Multiple PPP clients per ATM subinterface

Single Clients per ATM Subinterface

Figure 3 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, Chapter 1, Configuring ATM*.

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**

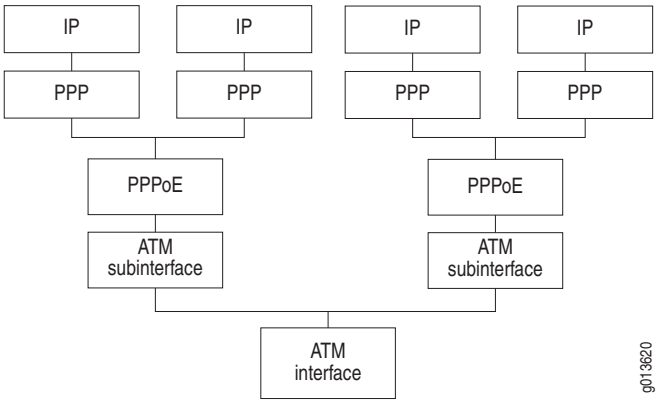
6. Assign a profile to the PPP interface.

   host1(config-subif)#**profile foo**

Multiple Clients per ATM Subinterface

Figure 4 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, Chapter 1, Configuring ATM*.

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**

Configuring AAA Profiles

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. For more information about **none**, see the section *Mapping User Requests Without a Valid Domain Name* on page 9. The domain name **default** indicates that no other match occurs. For more information about **default**, see the section *Mapping User Requests Without a Configured Domain Name* on page 9.

Allowing or Denying 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.

Configuration Example

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.

Using Domain Name Aliases

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.

Example 1 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.

Example 2 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.

aaa profile

- Use to configure a new AAA profile.
- Example

  host1(config)#**aaa profile boston123**

- Use the **no** version to delete the AAA profile.

allow

- Use to specify the domain name(s) that you want to be allowed access to AAA authentication.
- This command does not indicate that the user will be granted access; it is simply the first access point to AAA authentication.
- Using this command does not implicitly deny all other domains.
- Example

  host1(config-aaa-profile)#**allow xyz.com**

- Use the **no** version to negate the command.

deny

- Use to specify the domain name(s) that you want to be denied access to AAA authentication.
- Example

  host1(config-aaa-profile)#**deny xyz.com**

- Use the **no** version to negate the command.

ppp aaa-profile

- Use to assign an AAA profile to static and dynamic, multilink and nonmultilink PPP interfaces.
- The PPP application associates the AAA profile with the interface and passes the AAA profile to AAA for authentication.
- If an AAA profile is deleted after it has been assigned to an interface, AAA will deny the authentication and log a message.
- When you remove an AAA profile, it does not remove any corresponding bindings between PPP interfaces or interface profiles and the AAA profile. If an AAA profile with the same name is added, the interface cannot authenticate until the AAA profile is reassigned.

NOTE: Although an AAA profile and an interface profile have similar functionality, they are not related and should be treated differently.

- Example

  host1(config-if)#**ppp aaa-profile westford24**

- Use the **no** version to remove the AAA profile assignment.

translate

- Use to map the original domain name to the mapped domain name for domain map lookup.
- This command allows you to group multiple domain names into a single domain name (that is, to use aliases).
- You can use this command to partition PPP subscribers with the same domain into separate domains, based on the PPP interface. By doing this, you do not cause modification of the user's name or domain.
- Example

  host1(config-aaa-profile)#**translate abc.com xyz.com**

- Use the **no** version to negate the command.

Manually Setting NAS-Port-Type Attribute

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**

aaa profile

- Use to create and configure a AAA profile.
- Example

  host1(config)#**aaa profile nasPortType**

- Use the **no** version to delete the AAA profile.

nas-port-type atm

- Use to specify the RADIUS NAS-Port-Type attribute (61) for ATM interfaces. You can set the attribute to:
  - *value*—Number in the range 0–65535
  - **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
  - **adsl-dmt**—Asymmetric DSL, discrete multitone (DMT)
  - **cable**
  - **iapp**—Inter Access Point Protocol (IAPP)
  - **idsl**—ISDN DSL
  - **sdsl**—Symmetric DSL
  - **wireless-1x-ev**—Wireless 1xEV
  - **wireless-80211**—Wireless 802.11
  - **wireless-cdma**—Wireless code division multiple access (CDMA)
  - **wireless-other**
  - **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
  - **xdsl**—DSL of unknown type

- Example

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

- Use the **no** version to remove the NAS-Port-Type setting for ATM interfaces.

nas-port-type ethernet

- Use to specify the RADIUS NAS-Port-Type attribute (61) for Ethernet interfaces. You can set the attribute to:
  - *value*—Number in the range 0–65535
  - **cable**
  - **iapp**—IAPP
  - **wireless-1x-ev**—Wireless 1xEV
  - **wireless-80211**—Wireless 802.11
  - **wireless-cdma**—Wireless CDMA
  - **wireless-other**
  - **wireless-umts**—Wireless UMTS
- Example

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

- Use the **no** version to remove the NAS-Port-Type setting for Ethernet interfaces.

Service-Description Attribute

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**

aaa profile

- Use to create and configure a AAA profile.
- Example

  host1(config)#**aaa profile xyzCorpPro2**

- Use the **no** version to delete the AAA profile.

service-description

- Use to specify a description that is associated with the AAA profile. The description can be transmitted to RADIUS in the Service-Description attribute (26-53)
- The service description can be a maximum of 64 characters.
- Example

  host1(config-aaa-profile)#**service-description service11**

- Use the **no** version to remove the service description for the profile.

Using RADIUS Route-Download Server to Distribute Routes

The JUNOSe RADIUS route-download server provides periodic automatic distribution of IPv4 static 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*]
The route-download server accepts downloaded routes in either the Framed-Route attribute (RADIUS attribute 22) or the Cisco-AVpair attribute (Cisco VSA 26-1).

Downloaded Route Format Examples

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”

Cisco-AVPair (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”

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

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:

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 dl1456atl 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:                 dl1456atl
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
```

aaa route-download

- Use to enable the RADIUS route-download server on the router and to configure parameters for the server. You can configure the following parameters:
  - **download interval**—The amount of time the route-download server waits between route download operations. The newly created server downloads routes as soon as the IP protocol is active on the virtual router that performs the route download operation, and then repeats the download operation every 720 minutes by default. You can set a download interval in the range 1–1440 minutes.
  - **retry-interval**—The amount of time the server waits after a download failure before attempting another route download. You can set the retry interval in the range 1–60 minutes. The default interval is 10 minutes.

NOTE: If the download interval is less than the retry interval, the server ignores the retry interval setting.

  - **cost**—The cost of a downloaded route. You can specify a cost in the range 1–254. The default cost is 2.
  - **tag**—The tag assigned to a downloaded route. You can specify a tag in the range 1–4294967295. The default tag is 0.
  - **base-user-name**—The virtual router that is used for route-download requests. The default name is the router hostname.
  - **password**—The password used in RADIUS Access-Request messages for route-download requests. You can specify from 1 through 32 alphanumeric characters. The default password is juniper.
  - **synchronization**—The time that the server starts the route download operation each day. You specify the time in 24-hour format, for example 03:45:00.

- Example

  host1(config)#**aaa route-download 1200 retry-interval 25 password dl1456atl synchronization 03:45:00**

- Use the **no** version to disable the route-download server.

aaa route-download now

- Use to specify that the RADIUS route-download server immediately restart the route download operation.
- If a download is currently in progress when you issue this command without the **force** keyword, the in-progress download continues until complete. No additional download is started.
- Use the **force** keyword to start an immediate download; a currently running download is interrupted. The download is not retried if it fails.
- Use the **adjust-scheduler** keyword to restart the configured download interval from the time of this download. However, if the download fails, the download interval is not changed and the download is not retried.
- Example

  host1#**aaa route-download now force adjust-scheduler**

- There is no **no** version.

aaa route-download suspend

- Use to temporarily suspend the RADIUS route-download server operation.
- Example

  host1#**aaa route-download suspend**

- Use the **no** version to restore the route download operation.

clear ip routes download

- Use to synchronize downloaded access routes and the routes that are installed in the routing tables of virtual routers.
- Use the following options to synchronize downloaded routes for a specific virtual router:
  - Specify a particular VRF whose downloaded routes you want synchronized. If you do not specify an optional VRF, the current virtual router is used.
  - Specify the IP address and IP mask that identifies the subset of downloaded routes that you want cleared in the routing table of the current virtual router or in the specified VRF.
  - Use the wildcard character (*****) to clear all downloaded routes in the routing table of the current virtual router or in the specified VRF.

- Use the following keywords to perform global clearing operations:
  - **all**—Clears all downloaded routes from all virtual routers and VRFs.
  - **reload**—Initiates a download of routes and then clear the routes from the routing table of all virtual routers and VRFs.

NOTE: Clear commands fail if the route-download server is in the process of downloading routes from the RADIUS server.

- Example 1—Clear all downloaded routes from the current virtual router

  host1#**clear ip routes download ***

- Example 2—Clear a subset of routes from a specific VRF

  host1#**clear ip routes download vrf NY12 192.168.50.102 255.255.0.0**

- Example 3—Clear all downloaded routes from all virtual routers and VRFs

  host1#**clear ip routes download all**

- There is no **no** version.

radius route-download server

- Use to configure a RADIUS route-download server and enter RADIUS Configuration mode. Specify the IP address of the RADIUS server that you want to download access routes.

NOTE: When the RADIUS route-download server is enabled, the router ignores the **radius rollover-on-reject enable** command—the **radius rollover-on-reject enable** command has no effect for a RADIUS route-download server.

- You can configure a single instance of the route downloader on the router.
- Example

  host1(config)#**radius route-download server 10.10.5.10**
  host1(config-radius)#

- Use the **no** version to delete the instance of the RADIUS route-download server.

Using the AAA Logical Line Identifier to Track Subscribers

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.

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.

RADIUS Attributes in Preauthentication Request

Table 6 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 6: 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
[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.

For more information about these attributes, see *Chapter 6, RADIUS Attribute Descriptions*.

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. For information, see **radius rollover-on-reject** on page 32.

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 **show aaa profile command** in *Chapter 2, Monitoring and Troubleshooting Remote Access*.

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 **show radius servers command** in *Chapter 2, Monitoring and Troubleshooting Remote Access*.

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

To display preauthentication statistics, use the **show radius pre-authentication statistics** command. For information, see **show radius statistics command** in *Chapter 2, Monitoring and Troubleshooting Remote Access*.

To display a count of preauthentication requests and responses, use the **show aaa statistics** command. For information, see **show aaa statistics command** in *Chapter 2, Monitoring and Troubleshooting Remote Access*.

aaa profile

- Use to configure a new AAA profile.
- Example

  host1(config)#**aaa profile boston123**

- Use the **no** version to delete the AAA profile.

key

- Use from RADIUS Configuration mode to configure the secret for a RADIUS preauthentication server.
- The server secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS preauthentication server. The router encrypts PPP PAP passwords using this text string.
- The default behavior is no server secret.
- Example

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

- Use the **no** version to remove the secret.

NOTE: The preauthentication request fails if you do not specify a key for the preauthentication server.

ppp aaa-profile

- Use to assign an AAA profile to static and dynamic, multilink and nonmultilink PPP interfaces.
- For more information about how to use this command, see **ppp aaa-profile** on page 65.
- Example

  host1(config-if)#**ppp aaa-profile preAuth**

- Use the **no** version to remove the AAA profile assignment.

pre-authenticate

- Use to configure an AAA profile to support RADIUS preauthentication.
- During preauthentication, the router sends an Access-Request message to a RADIUS preauthentication server to obtain an LLID for a subscriber. In response, the preauthentication server returns the LLID in the RADIUS Calling-Station-Id [31] attribute of an Access-Accept message.
- Example

  host1(config-aaa-profile)#**pre-authenticate**

- Use the **no** version to remove preauthentication support from the AAA profile.

radius pre-authentication server

- Use to specify the IP address of a RADIUS preauthentication server.
- This command accesses RADIUS Configuration mode, from which you can configure additional parameters for the RADIUS preauthentication server.

- Example

  host1(config)#**radius pre-authentication server 10.10.10.2**

- Use the **no** version to delete the instance of the RADIUS preauthentication server.

Troubleshooting Subscriber Preauthentication

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.

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.

For more information, see *Configuring SNMP Traps* on page 36.

Using VSAs for Dynamic IP Interfaces

Table 7 describes the VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS. For details, see *JUNOSe Link Layer Configuration Guide, Chapter 16, Configuring Dynamic Interfaces Using Bulk Configuration*.

Table 7: VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Ingress-Policy-Name	Specifies the name of the input (ingress) policy	26	len	10	sublen	string: *input-policy-name*
Egress-Policy-Name	Specifies the name of the output (egress) policy	26	len	11	sublen	string: *output-policy-name*
Ingress-Statistics	Indicates whether statistics are collected on input	26	12	12	6	integer: 0 – disable, 1 – enable
Egress-Statistics	Indicates whether statistics are collected on output	26	12	13	6	integer: 0 – disable, 1 – enable
QoS-Profile-Name	Specifies the name of the QoS profile to attach to the interface	26	len	26	sublen	string: *qos-profile-name*

To use the VSAs shown in Table 7:

- Specify the policy, or one or more QoS VSAs in the desired RADIUS user entries.
- Create the ingress or egress policy, or the QoS profile. Policies minimally consist of one or more policy commands and may include classifier control lists and rate limit profiles. See the *JUNOSe Policy Management Configuration Guide* for more information about policies and policy routing. See the *JUNOSe Quality of Service Configuration Guide* for information about creating QoS profiles.

When a dynamic interface is created according to a profile, the router checks with RADIUS to determine whether an input or output policy or a QoS profile must be applied to the interface. The VSA, if present, provides the name, enabling policy or QoS profile lookup. If found, the policy or QoS profile is applied to the dynamic interface.

The router also determines whether the creation profile specifies any policies to be applied to the interface. Policies specified by the RADIUS VSA supersede any specified by the profile, as described in the following example:

> The RADIUS user entry includes an Ingress-Policy-Name VSA that specifies the policy input5. The profile specifies two policies, input7 and output1. In this case, the RADIUS-specified input policy (input5) and the profile-specified output policy (output1) are applied to the dynamic interface.

For information about assigning policies via profiles, see the *JUNOSe Policy Management Configuration Guide*. Only attributes assigned by RADIUS appear in RADIUS Acct-Start messages. RADIUS attributes specified by a profile for dynamic interfaces do not appear in RADIUS Acct-Start messages because the profile is not active when the Acct-Start message is generated. These attributes appear in RADIUS Acct-Stop messages for a profile that is active when the session is terminated.

Traffic Shaping for PPP over ATM Interfaces

The router supports the configuration of traffic shaping parameters for PPP over ATM (PPPoA) via domain-based profiles and RADIUS. In connection with this feature, Table 8 describes VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS.

Table 8: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Service-Category	Specifies the type of service	26	12	14	6	integer: 1 – UBR 2 – UBR PCR 3 – NRT VBR 4 – CBR 5 – RT VBR
PCR	Specifies the value for the peak cell rate (PCR)	26	12	15	6	integer

Table 8: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
SCR	Specifies the value for the sustained cell rate (SCR)	26	12	16	6	integer
MBS	Specifies the maximum burst size (MBS)	26	12	17	6	integer

To configure traffic-shaping parameters for PPPoA via domain maps, use the **atm** command in Domain Map Configuration mode.

atm

- Use to configure traffic-shaping parameters for PPPoA.
- Use one of the following keywords to select the traffic category to configure:
  - **ubr**—Unspecified bit rate
  - **ubrpcr—**Unspecified bit rate with peak cell rate
  - **nrtvbr**—Non–real time variable bit rate
  - **rtvbr**—Real time variable bit rate
  - **cbr**—Constant bit rate
- Example

  host1(config)#**aaa domain-map atmTraffic**
  host1(config-domain-map)#**atm rtvbr 3897832145 3597861230 4294967295**

- Use the **no** version to remove the traffic-shaping configuration.

Mapping Application Terminate Reasons to 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 9 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 9: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)
2	Lost Carrier	DCD was dropped on the port
3	Lost Service	Service can no longer be provided; for example, the user's connection to a host was interrupted
4	Idle Timeout	Idle timer expired
5	Session Timeout	Subscriber reached the maximum continuous time allowed for the service or session
6	Admin Reset	System administrator reset the port or session

Table 9: Supported RADIUS Acct-Terminate-Cause Codes (continued)

Code	Name	Description
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

Configuration Example

This example describes a sample configuration procedure that creates custom mappings for PPP terminate reasons.

1. Configure the router to include the Acct-Terminate-Cause attribute in RADIUS Acct-Off messages.

```
host1(config)#radius include acct-terminate-cause acct-off enable
```

2. (Optional) Display the current PPP terminate-cause mappings.

```
host1(config)#run show terminate-code ppp
                                                                    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
 --More--
```

3. (Optional) Display all PPP terminate reasons.

```
host1(config)#terminate-code ppp ?
  authenticate-authenticator-timeout           Configure authenticate
                                               authenticator timeout
                                               translation
  authenticate-challenge-timeout               Configure authenticate
                                               challenge timeout translation
  authenticate-chap-no-resources               Configure authenticate chap no
                                               resources translation
  authenticate-chap-peer-authenticator-timeout Configure authenticate chap
                                               peer authenticator timeout
                                               translation
  authenticate-deny-by-peer                    Configure authenticate deny by
                                               peer translation
 --More--
```

4. Configure your customized PPP terminate-cause to RADIUS Acct-Terminate-Cause code mappings.

```
host1(config)#terminate-code ppp authenticate-authenticator-timeout radius 3
host1(config)#terminate-code ppp authenticate-challenge-timeout radius 4
```

5. Verify the new terminate-cause mappings.

```
host1(config)#run show terminate-code ppp
                                                                      Radius
  Apps          Terminate Reason              Description             Code
---------   --------------------------   --------------------------   ------
ppp         authenticate-authenticator   authenticate authenticator     3
            -timeout                      timeout
ppp         authenticate-challenge-tim   authenticate challenge tim     4
            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--
```

radius include acct-terminate-cause

- Use to include the Acct-Terminate-Cause attribute (RADIUS attribute 49) in RADIUS Acct-Off messages.
- You control inclusion of the Acct-Terminate-Cause attribute by enabling or disabling this command.

- Example

  host1(config)#**radius include acct-terminate-cause acct-off disable**

- Use the **no** version to restore the default, enable.

terminate-code

- Use to configure a customized mapping relationship between an application's terminate reason and a RADIUS Acct-Terminate-Cause code (RADIUS attribute 49).
- To set up the mapping, specify the following variables with this command:
  1. Specify the application where the terminate event occurs. You can specify **aaa**, **l2tp**, **ppp**, or **radius-client**.
  2. Specify the application's terminate reason that you want to map.
     - Use the question mark character (**?**) to display a list of the application's terminate reasons. For example:

       host1(config)#**terminate-code l2tp ?**

     - See *Chapter 7, Application Terminate Reasons* for a list of the default terminate reasons for the AAA, L2TP, PPP, and RADIUS client applications.
  3. Specify RADIUS as the translation application that is used for mapping. Then, specify the RADIUS Acct-Terminate-Cause code that you want to map to the application's terminate reason. See Table 9 on page 80 for a list of supported RADIUS codes.
- Example

  host1(config)#**terminate-code ppp authenticate-challenge-timeout radius 4**

- Use the **no** version to restore a default mapping, which are listed in *Chapter 7, Application Terminate Reasons*. For example:

  host1(config)#**no terminate-code aaa deny-address-allocation-failure radius**

Configuring Timeout

You can configure an idle or a session timeout. The values you set are the default values for PPP B-RAS users. Attributes returned by RADIUS override these default settings on a per-user basis.

aaa timeout

- Use to set either an idle or a session timeout.
- The range in seconds for an idle timeout is 300–86400.
- The range in seconds for a session timeout is a minimum of 1 minute (60 seconds) through a maximum of 366 days (31622400 seconds).

- These values can also be set by RADIUS, where the range is not enforceable. PPP and L2TP will round the timeout values from RADIUS as follows:
  - If the session timeout is less than the minimum (60 seconds), that value is used.
  - If the idle timeout is less than the minimum (300 seconds), it is rounded up to the minimum.
  - If either timeout is greater than the maximum, it is rounded down to the maximum.
  - All other timeouts are rounded to the nearest minute.
- Example 1

  host1(config)#**aaa timeout idle 1200**

- Example 2

  host1(config)#**aaa timeout session 3600**

- For a session timeout, the router interprets the default value (indicated by **0**) to mean that the PPP or L2TP user session should be forced to the maximum session timeout, 366 days. This means that the duration of a PPP or an L2TP user session cannot exceed 366 days; once the maximum session timeout is reached, the router terminates the user session.
- Use the **no** version to restore the idle or session timeout to its default value, 0 (seconds).

Limiting Active Subscribers

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

aaa subscriber limit per-port

- Use to limit the number of active subscribers permitted on a port.
- Example

  host1(config)#**aaa subscriber limit per-port 2/0 20**

- Use the **no** version to return to the default value, 0 (zero).

aaa subscriber limit per-vr

- Use to limit the number of active subscribers permitted on a virtual router.
- Because profiles are applied to subscribers after the PPP authentication phase, subscribers that have their VR context specified by profiles are not denied access. Instead, when IP notifies AAA of the subscribers VR context, AAA checks limits. If the subscriber exceeds the VR limit, AAA revokes the subscriber's access and logs out the subscriber.
- Example

  host1:vr17(config)#**aaa subscriber limit per-vr 20**

- Use the **no** version to return to the default value, 0 (zero).

Notifying RADIUS of AAA Failure

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.

aaa accounting acct-stop on-aaa-failure

- Use to cause the router to send an Acct-Stop message if a user fails AAA, but RADIUS grants access.
- Example

  host1:vr17(config)#**aaa accounting acct-stop on-aaa-failure disable**

- Use the **no** version to return to the default value, enabled.

aaa accounting acct-stop on-access-deny

- Use to cause the router to issue an Acct-Stop message if RADIUS denies access.
- Example

  host1:vr17(config)#**aaa accounting acct-stop on-access-deny enable**

- Use the **no** version to return to the default value, disabled.

Configuring the SRC Client

The JUNOSe software has an embedded client that interacts with the Juniper Networks 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).

Table 10 provides common terms used in the COPS environment.

Table 10: 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.

Table 10: SRC Client and COPS Terminology (continued)

Term	Description
SRC	Session and Resource Control (SRC) software, formerly the Service Deployment System (SDX) software; functions as a COPS PDP.
XDR	External Data Representation Standard; a standard for the description and encoding of data. XDR can be used to transfer data between computers.

The JUNOSe software's 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.

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). The JUNOSe software's COPS-PR support uses a proprietary PIB. The proprietary PIB consists of a series of tables designed to replicate and enhance the XDR functionality that is supported in previous JUNOSe software releases, including the proprietary accounting and address assignment mechanisms. The XDR-encoded commands for the SRC software continue to be supported.

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

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 either BER-encoded information exchange for COPS-PR or XDR exchange for COPS.

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

   host1(config)#**sscc transportRouter chicago**

5. (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**

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

   host1(config)#**sscc sourceInterface atm 3/0**

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

   host1(config)#**sscc retryTimer 120**

sscc address

- Use to configure the SRC client with the IP addresses of the SAEs and the ports on which the SAEs listen for activity.
- You can specify primary, secondary, and tertiary SAEs, and the port numbers on which each listens for activity. By default, the SAE listens on port 3288.
- Example

  host1(config)#**sscc primary address 192.168.128.10 port 3288**

- Use the **no** version to remove a specific SAE (primary, secondary, or tertiary) from the list of SAEs.

sscc enable

- Use to enable the SRC client's COPS support in the router.
- Use with the **cops-pr** keyword to enable COPS-PR support; omit the **cops-pr** keyword to enable XDR-based COPS support.
- Example

  host1(config)#**sscc enable cops-pr**

- Use the **no** version to disable the feature.

sscc protocol ipv6

- Use to configure IPv6 support on the SRC client. IPv6 support enables policy and QoS configuration on IPv6 interfaces. The IPv6 support is in addition to the default IPv4 support.
- The SRC client does not support IPv6 policy and QoS configuration when in the XDR mode.
- Example

  host1(config)#**sscc protocol ipv6**

- Use the **no** version to disable IPv6 support on the SRC client.

sscc retryTimer

- Use to specify the delay period (in the range 5–300 seconds) during which the SRC client waits for a response from the SAE.
- If only a primary SAE is configured, the client resends the request to the primary SAE.

- The client attempts to connect to a tertiary SAE only if both the primary and secondary SAEs are unavailable. For example, if the client is connected to the secondary SAE when the delay period expires, the client first tries to connect to the primary SAE before trying the tertiary SAE. The client waits for the length of the delay period before each attempt.
- Example

  host1(config)#**sscc retryTimer 90**

- Use the **no** version to restore the default value, 90 seconds.

sscc sourceAddress

- Use to specify a fixed source address for the TCP/COPS connection created for an SRC client session. This is the local address.
- If you do not specify a source address, the TCP/COPS connection is not bound to a specific source (that is, local) address.
- Example

  host1(config)#**sscc sourceAddress 10.9.123.8**

- Use the **no** version to remove the specified address.

sscc sourceInterface

- Use to specify a fixed source interface for the TCP/COPS connection created for an SRC client session. This is a local interface.
- You may need to set a source interface in cases where a firewall, access control list, or policy configuration exists; and it is important to know what the interface is, or you need to set the interface independently from other protocols that have conflicting requirements.
- If you do not specify a source interface, the TCP/COPS connection is not bound to a specific source (that is, local) interface.
- Example

  host1(config)#**sscc sourceInterface atm 3/0**

- Use the **no** version to remove the source interface.

sscc transportRouter

- Use to specify on which router the TCP/COPS connection is to be established.
- The router can be the same as or different from the router the SRC client session is created in and associated with.
- If you do not specify the transport router for an SRC client session, the transport router defaults to the router associated with the session.
- Example

  host1(config)#**sscc transportRouter chicago**

- Use the **no** version to remove the specified SRC client transport router.