ERICSSON

Configuring Authentication, Authorization, and Accounting

SYSTEM ADMINISTRATOR GUIDE

61/1543-CRA 119 1170/1-V1 Uen K

Contents

1 Overview

This document provides an overview of the authentication, authorization, and accounting (AAA) features of the SmartEdge router and describes the tasks used to configure, monitor, and administer AAA. This document also provides AAA configuration examples.

Note: In the following descriptions, the term *controller card* refers to the Cross-Connect Route Processor (XCRP4) Controller card. The term controller carrier card refers to the controller functions on the carrier card in the SmartEdge 100 chassis.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

1.1 Authentication

The following sections describe authentication features for administrators and subscribers.

1.1.1 Administrators

By default, the SmartEdge router configuration performs administrator authentication. You can also authenticate administrators through database records on a Remote Authentication Dial-In User Service (RADIUS) server, through a Terminal Access Controller Access Control System Plus (TACACS+) server, or through one method, followed by another.

You must configure the IP address of a reachable RADIUS or TACACS+ server (or both) in the context in which the administrator is configured. For information about RADIUS and TACACS+, see *Configuring RADIUS* and *Configuring TACACS+* respectively.

You can set a maximum limit on the number of administrator sessions that can be simultaneously active in each context.

1.1.2 Subscribers

Authentication of Point-to-Point Protocol (PPP) subscribers now includes support for IPv4, IPv6, and dual-stack subscribers. Dual-stack subscribers run both IPv4 and IPv6. For information on IPv6 subscribers, refer to *Configuring IPv6 Subscriber Services*. Authentication requests do not indicate if a session is single or dual stack, but authentication responses do.

An IPv6 subscriber must be authorized through AAA before PPP negotiates connectivity and ND processes packets. If a protocol is not authorized, PPP does not negotiate that protocol with a client, even when the PPP negotiation process is initiated by a client.

1.1.2.1 Authentication Options

By default, the operating system configuration performs subscriber authentication. You can also authenticate subscribers through database records on a RADIUS server, or through multiple methods.

When the IP address or hostname of the RADIUS server is configured in the operating system local context, *global* RADIUS authentication is performed. That is, although subscribers may be configured in a nonlocal context, subscribers in nonlocal contexts are authenticated through the RADIUS server configured in the local context. With global RADIUS authentication, the RADIUS server returns the Context-Name vendor-specific attribute (VSA) indicating the name of the particular context to which subscribers are bound.

When the IP address or hostname of the RADIUS server is configured in a context other than the local context, *context-specific* RADIUS authentication is performed; that is, only subscribers bound to the context in which the RADIUS server's IP address or hostname is configured are authenticated.

You can also configure the SmartEdge router to attempt authentication through a RADIUS server configured in the nonlocal context first, and then to a RADIUS server configured in the local context if the first server is unavailable. Or, you can configure the SmartEdge router to attempt authentication through a RADIUS server configured in a nonlocal context, and then to the SmartEdge router configuration.

AAA includes the following Layer 2 Tunneling Protocol (L2TP) attribute-value pairs (AVPs), RADIUS standard attributes, and vendor-specific attributes (VSAs) provided by Ericsson in RADIUS Access-Request messages for L2TP network server (LNS) subscribers that are authenticated using RADIUS:

- Tunnel-Client-Endpoint (66)
- Tunnel-Server-Endpoint (67)
- Acct-Tunnel-Connection (68)
- Tunnel-Assignment-ID (82)

- Tunnel-Client-Auth-ID (90)
- Tunnel-Server-Auth-ID (91)
- Tunnel-Function (VSA 18)
- Tx-Connect-Speed (L2TP AVP 24)
- Rx-Connect-Speed (L2TP AVP 38)

If you have IPv6 PPP subscriber sessions, the following standard RADIUS attributes and Ericsson VSAs are supported:

- NAS-IPv6-Address (95)
- Framed-Interface-Id (96)
- Framed-IPv6-Prefix (97)
- Framed-IPv6-Route (99)
- Framed-IPv6-Pool (100)
- Delegated-IPv6-Prefix (123)
- RB-IPv6-DNS (207)
- RB-IPv6-Option (208)
- Delegated-Max-Prefix (212)

For more information about RADIUS standard attributes and vendor VSAs provided by Ericsson AB, see *RADIUS Attributes*. For more information about L2TP AVPs, see *Configuring L2TP*.

1.1.2.2 Maximum Subscriber Sessions

You can set a maximum limit on the number of subscriber sessions that can be simultaneously active in a given context and for all configured contexts.

1.1.2.3 Limit Subscriber Services

You can limit the services provided to subscribers based on volume of traffic. You can monitor volume-based services in the upstream and downstream directions independently, separately, or aggregated in both directions. However, you cannot simultaneously monitor aggregated traffic and either upstream or downstream traffic.

Volume limits are imposed by the RADIUS VSA 113 in Access-Accept and Accounting-Request messages.

AAA supports inbound and outbound traffic counters, as well as an aggregated counter of both incoming and outgoing traffic. If the aggregated counter

exceeds the configured value for aggregated traffic limit, AAA sends a RADIUS accounting message or tears down the subscriber session, depending on the configured action to perform.

If the RADIUS attribute does not include the direction to which the limit is applied, the downstream direction is assumed. If no limit is included, the traffic volume is unlimited in both directions and is not monitored. If a limit of 0 is configured for a direction, traffic is treated as unlimited in that direction and is not monitored.

VSA 113 is also supported in a subscriber reauthorize Access-Accept message.

1.1.2.4 Binding Order

If a subscriber circuit has been configured with a dynamic binding, using the **`bind authentication`** command (in the circuit's configuration mode), AAA uses subscriber attributes in messages received during subscriber authentication to determine which IPv4 address (and the associated interface) to use when binding the subscriber circuit.

By default, the SmartEdge router considers L2TP attributes before considering RADIUS attributes. You can reverse this order so that the IPv4 address provided in the RADIUS record is used before one provided by L2TP.

1.1.2.5 IP Address Assignment

By default, the SmartEdge router uses a round-robin algorithm to allocate subscriber IPv4 addresses from the IP pool. You can also configure the router to use a first-available algorithm.

AAA typically assigns an IPv4 address to a Point-to-Point Protocol (PPP) subscriber from an IP pool after receiving an Access-Accept packet from a RADIUS server. However, you can configure AAA to provide an IPv4 address from an IP pool in the Framed-IP-Address attribute in the RADIUS Access-Request packet. This IPV4 IP address is provided to the RADIUS server as a "hint" that it is a preferred address. If there are no unassigned IPv4 addresses in the pool, the authentication request is sent without an IPv4 address.

The RADIUS server can accept the address or not; Table 1 lists the RADIUS server responses and the corresponding router actions.

Table 1 SmartEdge Router and RADIUS Server Actions

RADIUS Server Response	SmartEdge Router Corresponding Action
Framed-IP-Address attribute contains 255.255.255.254, 0.0.0.0, or is missing.	SmartEdge router assigns preferred IPv4 address.
Framed-IP-Address attribute contains a different IPv4 address.	SmartEdge router assigns the IPv4 address in the Framed-IP-Address attribute and returns the preferred IPv4 address to its pool.

1.2 Authorization and Reauthorization

The following sections describe authorization and reauthorization features.

1.2.1 CLI Commands Authorization

You can specify that commands with a matching privilege level (or higher) require authorization through TACACS+.

1.2.2 Dynamic Subscriber Reauthorization

When subscribers request new or modified services during active sessions, the requests can be translated to changes that are applied during the active session through dynamic subscriber reauthorization. Reauthentication occurs without PPP renegotiation and without interrupting or dropping the active session.

1.3 Accounting

The following sections describe accounting features.

1.3.1 CLI Commands Accounting

You can configure the SmartEdge router so that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher).

1.3.2 Administrator Accounting

You can configure administrator accounting, which tracks messages for administrator sessions; the messages are sent to a RADIUS or TACACS+ server.

1.3.3 Subscriber Accounting

You can configure subscriber accounting, which tracks messages for subscriber sessions; the messages are sent to a RADIUS accounting server. Use the **aaa accounting subscriber** command with the **radius** keyword to configure subscriber accounting. When the IP address or hostname of the RADIUS accounting server is configured in the SmartEdge router local context, global authentication is performed. That is, although subscribers are configured in a non-local context, accounting messages for subscribers sessions in the context are sent through the RADIUS accounting server configured in the local context. When using global RADIUS subscriber accounting, configuring global RADIUS subscriber authentication is required.

Note: Configuring the **global** keyword with the **aaa accounting subscriber** command allows you to enable global RADIUS subscriber accounting without requiring that global authentication also be performed. For more information, see the **aaa accounting subscriber** command.

When the IP address or hostname of the RADIUS accounting server is configured in a context other than the local context, context-specific accounting is performed; that is, accounting messages are sent only for subscribers bound to the context in which the RADIUS accounting server IP address or hostname is configured.

You can configure two-stage accounting—the SmartEdge router sends accounting messages to a RADIUS accounting server configured in the non-local context and to a RADIUS accounting server configured in the local context. For example, a copy of the accounting data can be sent to a both a wholesaler's and an upstream service provider's RADIUS accounting server, so that end-of-period accounting data can be reconciled and validated by both parties.

You can also specify the error conditions for which the SmartEdge router suppresses the sending of accounting messages to a RADIUS accounting server.

1.3.4 L2TP Accounting

You can configure L2TP accounting, which tracks messages for L2TP tunnels, or sessions in L2TP tunnels; the messages are sent to a RADIUS accounting server. When the IP address or hostname of the RADIUS accounting server is configured in the SmartEdge router local context, global accounting is performed. When the IP address or hostname of the RADIUS accounting server is configured in a context other than the local context, context-specific accounting is performed. You can also configure two-stage accounting.

The SmartEdge router sends just a single `accounting on` message when more than one type of RADIUS accounting is enabled. For example, if you enable both subscriber accounting and L2TP accounting, the router sends only one “accounting on” message to each RADIUS accounting server, even if you

enable L2TP accounting at a later time. Similarly, the “accounting off” message is not sent until you have disabled all types of RADIUS accounting.

Note: Configuring the **`global`** keyword with the **`aaa accounting l2tp session`** command allows you to enable global RADIUS accounting for sessions in L2TP tunnels without requiring that global authentication also be performed. For more information, see the **`aaa accounting l2tp`** command.

If a subscriber session cannot be tunneled to a specific L2TP network server (LNS) or to an LNS in a group of L2TP peers, or if the SmartEdge router has received a Link Control Protocol (LCP) termination request from the subscriber before session establishment is complete, the Acct-Session-Time attribute is set to *0.*

1.4 AAA Route Download Overview

The SmartEdge router allows you to configure and advertise IPv4 access routes before the routes have been assigned to subscribers. Pre-provisioning access routes helps eliminate routing protocol scalability issues or delays when the protocol is converging or when a large number of subscribers are being simultaneously activated. More than one RADIUS server can be designated as a route download server. When defining a route download server, RADIUS server redundancy operates in the normal way.

When this feature is enabled, the SmartEdge router periodically sends a RADIUS Access-Request message to the RADIUS server acting as a route download server, requesting to download routes. To respond, the RADIUS server sends an Access-Accept message containing a set of routes within the RFC-specified RADIUS packet length, which the SmartEdge router downloads. The SmartEdge router repeats the request until all the routes have been downloaded; the RADIUS server signals completion by rejecting the Access-Request message. Once all the routes have been downloaded successfully, the SmartEdge router installs the access routes in its RIB. If the download fails at any point, all the routes are discarded; the SmartEdge router never installs an incomplete batch of routes into its RIB.

A set of download requests is sent on a periodic basis, beginning at a configured time of day and repeating at configured intervals thereafter. Routes are carried in the Framed-Route attribute (standard attribute 22), which must be formatted as specified in RFC 2865, Remote Authentication Dial In User Service (RADIUS). The metric field in the Framed-Route attribute is optional. The SmartEdge router uses the Context-Name attribute (VSA attribute 4) to identify the context into which to download the route.

This feature assumes that routes downloaded from the RADIUS route download server has a more specific prefix than the prefix of the subscriber route. The SmartEdge router does not check for configuration errors in this regard.

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

To configure, administer, and troubleshoot AAA, perform the tasks described in the following sections.

2.1 Configure Global AAA

To configure global attributes for AAA, perform the tasks in the following sections.

2.1.1 Limit the Number of Active Administrator Sessions

To limit the number of administrator sessions that can be simultaneously active in a given context, perform the task described in Table 2.

Table 2 Limit the Number of Active Administrator Sessions

Task	Root Command	Notes
Limit the number of administrator sessions that can be simultaneously active in a given context.	*aaa authentication administrator*	Enter this command in context configuration mode. To set the limit, use the **`maximum sessions`** ***`num-sess`*** construct.

2.1.2 Limit the Number of Active Subscriber Sessions

To limit the number of subscriber sessions that can be simultaneously active, perform the task described in Table 3.

Table 3 Limit the Number of Active Subscriber Sessions

Task	Root Command	Notes
Limit the number of subscriber sessions that can be simultaneously active in a given context.	*aaa maximum subscriber*	Enter this command in context configuration mode.

2.1.3 Prevent Subscriber Session Authentication Once Session Limit is Reached

To prevent a new session from being authenticated when the maximum configured number of sessions has been reached, perform the task described in Table 4.

Table 4 Prevent Subscriber Session Authentication Once Session Limit is Reached

Task	Root Command	Notes
Prevent a new subscriber session from being authenticated when the maximum configured number of sessions has been reached.	*aaa global suppress-authentication slid-session-limit*	Enter this command in global configuration mode.

2.1.4 Enable a Direct Connection for Subscriber Circuits

To enable a direct connection for subscriber circuits, configure the SmartEdge router to install the route specified by the RADIUS Framed-IP-Netmask attribute. This configuration is described in Table 5.

Table 5 Enable a Direct Connection for Subscriber Circuits

Task	Root Command	Notes
Enable use of the RADIUS Framed-IP-Netmask attribute to install the route to a remote router.	*aaa provision route*	Enter this command in context configuration mode.

2.1.5 Define Structured Username Formats

To define one or more schema for matching the format of structured usernames (subscriber and administrator names), perform the task described in Table 6.

Table 6 Define Structured Username Formats

Task	Root Command	Notes
Define one or more schema for matching the format of structured usernames.	*aaa username-format*	Enter this command in global configuration mode. If no username formats are explicitly defined, the SmartEdge router checks the default format, username@domain-name, for a match.

2.1.6 Username Authentication

To require a username for authentication, perform the task described in Table 7.

Table 7 Require Username for Authentication

Task	Root Command	Notes
Specify that the User-Name attribute is required in Access-Request messages.	*aaa global reject empty-username*	Enter this command in global configuration mode. If no value is specified for the User-Name attribute, AAA suppresses the Access-Request message, and subscriber authentication fails.

By default, the SmartEdge router sends Access-Request messages to the RADIUS server, regardless of whether a username is specified.

2.1.7 Acknowledge RSE Service Activation via CoA on Stack Mismatch

To acknowledge an RSE service activation via CoA even if it is applying an RSE service containing both IPv4 and IPv6 attributes to a single stack IPv4 subscriber, perform the task described Table 8.

Table 8 Acknowledge RSE Service Activation via CoA on Stack Mismatch

Task	Root Command	Notes
Specify that RSE service activation via CoA will be acknowledged even if it is applying an RSE service containing both IPv4 and IPv6 attributes to a single stack IPv4 subscriber.	*aaa global coa ignore rse-attr-stack-mismatch*	Enter this command in global configuration mode.

2.2 Configure Authentication

To configure authentication, perform the tasks described in the following sections.

2.2.1 Configure Administrator Authentication

To configure administrator authentication, perform the task described in Table 9.

Table 9 Configure Administrator Authentication

Task	Root Command	Notes
Configure administrator authentication.	*aaa authentication admin istrator*	Enter this command in context configuration mode. You have the option to configure either the console port or a vty port for each specified authentication method. By default, both ports are enabled for use. Use either the console or vty keyword as needed.

2.2.2 Configure Subscriber Authentication

To configure subscriber authentication, perform the tasks described in the following sections.

2.2.2.1 Configure IP Address Assignment

To configure the algorithm the SmartEdge router uses to assign subscriber IPv4 address, perform the task described in Table 10.

Table 10 Configure IPv4 or IPv6 IP Address Assignment

Task	Root Command	Notes
Change the logic the SmartEdge router uses to allocate subscriber IP addresses from the default algorithm (round-robin) to a first-available algorithm.	*aaa ip-pool allocation first-available*	Enter this command in global configuration mode.

2.2.2.2 Enable the Assignment of Preferred IP Addresses

To enable the SmartEdge router to provide a RADIUS server with preferred IP addresses when performing subscriber authentication, perform the task described in Table 11.

Table 11 Enable the Assignment of Preferred IP Addresses

Task	Root Command	Notes
Enable the SmartEdge router to provide the RADIUS server with preferred IP addresses from unnamed IP pools.	*aaa hint ip-address*	Enter this command in context configuration mode.

2.2.2.3 Change the Default Order for Determining Subscriber IP Addresses

To change the default order for determining the IP address (and its interface) to be used for binding a subscriber circuit, perform the task in Table 12.

Table 12 Change the Default Order for Determining Subscriber IP Addresses

Task	Root Command	Notes
Change the default order for determining the IP address for binding a subscriber circuit.	*aaa provision binding-order*	Enter this command in context configuration mode.

2.2.2.4 Configure Global RADIUS Authentication

To configure global RADIUS authentication, perform the tasks described in Table 13.

Table 13 Configure Global RADIUS Authentication

Task	Root Command	Notes
Enable global RADIUS authentication.	*aaa global authentication subscriber*	Enter this command in global configuration mode. At least one RADIUS server IP address or hostname must be configured in the local context; for more information, see *Configuring RADIUS*.
Authenticate subscribers in the current context through one or more RADIUS servers with IP addresses or hostnames configured in the local context.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **`global`** keyword with this command.

2.2.2.5 Configure Context-Specific RADIUS Authentication

To authenticate subscribers using one or more RADIUS servers with IP addresses or hostnames configured in the current context, perform the task described in Table 14.

Table 14 Configure Context-Specific RADIUS Authentication

Task	Root Command	Notes
Configure context-specific RADIUS authentication.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **radius** keyword with this command to configure RADIUS authentication. At least one RADIUS server IP address or hostname must be configured in the current context; for more information, see *Configuring RADIUS*.

2.2.2.6 SmartEdge Router (Local) Authentication

To authenticate subscribers through the SmartEdge router configuration, perform the task described in Table 15.

Table 15 Configure SmartEdge Router Configuration Authentication

Task	Root Command	Notes
Configure SmartEdge router configuration authentication.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **local** keyword with this command to configure RADIUS authentication.

2.2.2.7 Configure DHCPv6 Interface Authentication

Enable AAA to authenticate subscribers through the SmartEdge router local database. Subscribers are authenticated according to parameters set in the subscriber profile for the current context. In the subscriber local context, to configure an interface as a DHCPv6 interface, AAA must be enabled to provide subscriber authentication. To authenticate subscribers through a DHCPv6 server, perform the tasks described in Table 14.

Table 16 Configure SmartEdge Router DHCPv6 Interface Authentication

Task	Root Command	Notes
Configure an interface to be a DHCPv6 server interface.	**dhcpv6 server interface**	The DHCPv6 server uses the primary IPv6 address of the interface as the server IP address.
Enable AAA to authenticate subscribers through the SmartEdge router local database or RADIUS.	**aaa authentication subscriber local** or **aaa authentication subscriber radius**	Subscribers are authenticated according to parameters set in the subscriber profile for the current context.

When the SmartEdge router is configured to provide dual-stack and IPv6 subscriber services, DHCPv6 requests AAA for prefix delegation. In response to the DHCPv6 request, AAA returns one or more prefixes. For more information on DHCPv6 configuration, refer to *Configuring DHCP*. For an example of an end-to-end IPv6 configuration to see where AAA subscriber authentication is required, refer to *Configuring IPv6 Subscriber Services*.

2.2.2.8 Configure Context-Specific RADIUS and Global RADIUS Authentication

To configure context-specific RADIUS authentication, followed by global RADIUS authentication, perform the tasks described in Table 17.

Table 17 Configure Context-Specific RADIUS and Global RADIUS Authentication

Task	Root Command	Notes
Enable global RADIUS authentication.	*aaa global authentication subscriber*	Enter this command in global configuration mode. At least one RADIUS server IP address or hostname must be configured in the local context; for more information, see *Configuring RADIUS*.
Configure context-specific RADIUS followed by global RADIUS authentication.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **radius global** construct with this command.

2.2.2.9 Context-Specific RADIUS and SmartEdge Router (Local) Authentication

To authenticate subscribers using one or more RADIUS servers with IPv4 addresses or hostnames configured in the current context, followed by the SmartEdge router, perform the task described in Table 18.

Table 18 Configure Context-Specific RADIUS and SmartEdge Router Authentication

Task	Root Command	Notes
Configure context-specific RADIUS authentication, followed by SmartEdge router configuration authentication.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **radius** keyword followed by the **local** keyword with this command. At least one RADIUS server IP address or hostname must be configured in the current context; for more information, see *Configuring RADIUS*.

2.2.2.10 Configure a Last-Resort Authentication Context

To specify a context to attempt authentication of a subscriber when the domain portion of the subscriber name cannot be matched, perform the task described in Table 19.

Table 19 Configure a Last-Resort Authentication Context

Task	Root Command	Notes
Configure a last-resort authentication context.	*aaa last-resort*	Enter this command in global configuration mode.

2.2.3 Disable Subscriber Authentication

To disable authentication of subscribers in the current context, perform the task described in Table 20.

Table 20 Disable Subscriber Authentication

Task	Root Command	Notes
Disable subscriber authentication.	*aaa authentication subscriber*	Enter this command in context configuration mode. Use the **none** keyword with this command if subscriber authentication is not required, such as when Dynamic Host Configuration Protocol (DHCP) is used to obtain IPv4 addresses for subscriber hosts.

Caution!

Risk of security breach. If you disable subscriber authentication, individual subscriber names and passwords are not authenticated by the SmartEdge router, so IP routes and ARP entries within individual subscriber records are not installed. To reduce the risk, verify your network security setup before disabling subscriber authentication.

2.3 Configure Authorization and Reauthorization

To configure authorization and reauthorization, perform the tasks described in the following sections.

2.3.1 Configure CLI Commands Authorization

To specify that commands with a matching privilege level (or higher) require authorization through TACACS+, perform the task described in Table 21.

Table 21 Configure CLI Commands Authorization

Task	Root Command	Notes
Configure CLI commands authorization.	*aaa authorization commands*	Enter this command in context configuration mode. A TACACS+ server must be configured in the specified context; for more information, see *Configuring TACACS+*.

2.3.2 Configure L2TP Peer Authorization

To determine whether L2TP peers are authorized by the SmartEdge router (local) configuration or by a RADIUS server, perform the task described in Table 22.

Table 22 Configure L2TP Peer Authorization

Task	Root Command	Notes
Configure L2TP peer authorization.	*aaa authorization tunnel*	Enter this command in context configuration mode. By default, L2TP peers are authorized through the SmartEdge router configuration.

2.3.3 Configure Dynamic Subscriber Reauthorization

To configure dynamic subscriber reauthorization, perform the task described in Table 23.

Table 23 Configure Dynamic Subscriber Reauthorization

Task	Root Command	Notes
Configure dynamic subscriber reauthorization.	*aaa reauthorization bulk*	Enter this command in context configuration mode.

For reauthorization to take effect, vendor VSA 94 provided by Ericsson AB, Reauth-String, must be configured on the RADIUS server. Vendor VSA 95, Reauth-More, is only needed if multiple reauthorization records are used for one command; for example, if you have the following records, the **`reauthorize bulk 1`** command causes the RADIUS server to process reauthorization for **reauth-1@local** followed by **reauth-2@local:**

```
reauth-1@local

Password="redback"

Reauth-String="ID-type;subID;attr-num;attr-value;attr-num;attr-value...

Reauth-More=1


reauth-2@local

Password="redback"

Reauth-String="ID-type;subID;attr-num;attr-value;attr-num;attr-value...


Reauth_String

Attribute number: 94

Value: String

Format: "xxx"*

Send in Access-Request packet: No

Send in Accounting-Request packet: No

Receivable in Access-Request packet: Yes
```

```
Description: (SE)

* Format for Reauth String

"type;sub_id;attr#;attr_val;attr#;;attr#;attr_val;..."

(vsa_attr: vid-vsa_attr_#)

Reauth_More

Attribute number: 95

Value: integer

Format: 1

Send in Access-Request packet: No

Send in Accounting-Request packet: No

Receivable in Access-Request packet: Yes

Description: More reauth request is needed (SE)
```

For a list of the standard RADIUS attributes and vendor-specific attributes (VSAs) that are supported as part of the **Reauth-String** and details about them, see *RADIUS Attributes*.

2.4 Configure Accounting

To configure accounting, perform the tasks described in the following sections.

2.4.1 Configure CLI Commands Accounting

To specify that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher), perform the task described in Table 24.

Table 24 Configure CLI Commands Accounting

Task	Root Command	Notes
Configure CLI commands accounting.	*aaa accounting commands*	Enter this command in context configuration mode. A TACACS+ server must be configured in the specified context; see *Configuring TACACS+*.

2.4.2 Configure Administrator Accounting

To enable accounting messages for administrator sessions to be sent to the TACACS+ server, perform the task described in Table 25.

Table 25 Configure Administrator Accounting

Task	Root Command	Notes
Configure administrator accounting.	*aaa accounting administrator*	Enter this command in context configuration mode. A TACACS+ server must be configured in the specified context; see *Configuring TACACS+*.

2.4.3 Configure Subscriber Accounting

To configure subscriber accounting, perform the tasks described in the following sections.

2.4.3.1 Configure Global Subscriber Accounting

To configure global subscriber accounting, perform the tasks described in Table 26.

Note: You must configure local subscriber authentication; for more information, see Configure Global RADIUS Authentication earlier in this section. You must also configure at least one RADIUS accounting server in the local context; for more information, see *Configuring RADIUS*.

Table 26 Configure Global Subscriber Accounting

Task	Root Command	Notes
Enable global subscriber session accounting messages.	*aaa global accounting subscriber*	Enter this command in global configuration mode. Accounting messages for subscriber sessions in all contexts are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Table 26 Configure Global Subscriber Accounting

Task	Root Command	Notes
Enable global subscriber session accounting update messages.	*aaa global update subscriber*	Enter this command in global configuration mode. Updated accounting records for subscriber sessions in all contexts are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.
Enable global accounting messages for the **`reauthorize`** command.	*aaa global accounting reauthorization subscriber*	Enter this command in global configuration mode. Accounting messages for the **`reauthorize`** command issued in any context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.
Enable global accounting messages for subscriber session DHCP lease, DHCPv6 prefix delegation (PD), reauthorization, or ANCP events.	*aaa global accounting event*	Enter this command in global configuration mode. Accounting updates for DHCP lease, DHCPv6 PD, , IPv4 and IPV6 single-stack to dual-stack or dual-stack to single-stack transitions, reauthorization, or ANCP events for subscriber sessions in all contexts are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

2.4.3.2 Configure Context-Specific Subscriber Accounting

To configure context-specific subscriber accounting, perform the tasks described in Table 27. Enter all commands in context configuration mode.

Note: At least one RADIUS accounting server must be configured in the current context before any messages can be sent; for more information, see *Configuring RADIUS*.

Table 27 Configure Context-Specific Subscriber Accounting

Task	Root Command	Notes
Enable context-specific subscriber accounting messages.	*aaa accounting subscriber*	Accounting messages for subscriber sessions in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.
Enable context-specific subscriber session accounting update messages.	*aaa update subscriber*	Sends updated accounting records for subscriber sessions in the current context to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.
Enable context-specific accounting messages for the **`reauthorize`** command.	*aaa accounting reauthorization subscriber*	Accounting messages for the **`reauthorize`** command used in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.
Enable context-specific accounting messages for DHCP lease, DHCPv6 prefix delegation (PD), reauthorization information, or ANCP events.	*aaa accounting event*	Accounting messages for DHCP lease, DHCPv6 PD, IPv4 and IPV6 single-stack to dual-stack or dual-stack to single-stack transitions, reauthorization information, or ANCP events for subscriber sessions in the current context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.
Suppress accounting messages when subscriber sessions cannot be established.	*aaa accounting suppress-acct-on -fail*	Accounting messages are not sent to the RADIUS server when subscriber sessions cannot be established due to an authentication problem, a changed IP address, and so on.

2.4.3.3 Configure Two-Stage Subscriber Accounting

Two-stage accounting collects RADIUS accounting data on both global RADIUS servers and context-specific RADIUS servers.

To configure two-stage accounting for subscriber sessions, perform the tasks in Configure Subscriber Accounting and Configure Context-Specific Subscriber Accounting.

2.4.4 Configure L2TP Accounting

To configure L2TP accounting, perform the tasks described in the following sections.

2.4.4.1 Configure Global L2TP Accounting

To configure global L2TP accounting, perform the task described in Table 28.

Table 28 Configure Global L2TP Accounting

Task	Root Command	Notes
Configure global L2TP accounting.	*aaa global accounting l2tp-session*	Enter this command in global configuration mode. For all contexts, accounting messages for L2TP tunnels, or sessions in L2TP tunnels, are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

2.4.4.2 Configure Context-Specific L2TP Accounting

To configure context-specific L2TP accounting, perform the task described in Table 29.

Table 29 Configure Context-Specific L2TP Accounting

Task	Root Command	Notes
Configure context-specific L2TP accounting.	*aaa accounting l2tp*	Enter this command in context configuration mode. For the current context, accounting messages for L2TP tunnels, or sessions in L2TP tunnels, are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

2.4.4.3 Configure Two-Stage L2TP Accounting

Two-stage accounting collects RADIUS accounting data on both global RADIUS accounting servers and context-specific RADIUS accounting servers.

To configure two-stage accounting for subscriber sessions, perform the tasks in Configure Global L2TP Accounting and Configure Context-Specific L2TP Accounting.

2.5 Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

To administer and troubleshoot AAA features, perform the appropriate AAA operations task in Table 30. Enter all commands in exec mode.

Table 30 AAA Operations Tasks

Task	Root Command
Enable the generation of AAA debug messages.	*debug aaa*
Modify a subscriber attribute in real time during an active session, using the CLI.	*policy-refresh*
Modify a subscriber attribute in real time during an active session, using the RADIUS authentication process.	*reauthorize*
Test the communications link to a RADIUS server.	*test aaa*

2.6 Configure AAA Route Download

Before you can configure AAA route download, you must configure the AAA route-download server.

2.6.1 Configure the AAA Route-Download Server

To be able to configure a route-download server:

1. Use the *configure* command to access global configuration mode.
2. Use the *context* command to access context configuration mode.
3. Use the *radius route-download server* command to designate a RADIUS route download server, and configure the shared key (encrypted or not) and optional port. If the port is not specified, the default value of 1812 is used.

2.6.2 Configure Route-Download Capabilities

Once you have configured a route-download server, you can configure route-download functionality in context configuration mode:

1. Use the *radius route-download algorithm* command to specify the load-balancing algorithm to use when multiple servers are configured. By

default , the request is sent to the first available radius server. You can also configure round-robin load balancing.

2. Use the *radius route-download deadtime* command to specify the interval, in minutes, to consider a RADIUS route-download server unavailable before declaring it available again. The range is 0 to 65,535. If not specified, the server is never declared available again. The default deadtime value is 5 minutes.

3. Use the *radius route-download max-retries* command to specify the maximum number of times a route download request is retried. The range is 1 to 2,147,483,647. The default is 3.

4. Use the *radius route-download server-timeout* command to specify the interval, in seconds, to wait for a response from the RADIUS server before declaring it unavailable. The range is 1 to 2,147,483,647. If not specified, the server is never considered unavailable. The functionality is disabled by default.

5. Use the *radius route-download timeout* command to specify the interval, in seconds, to wait before retrying a request. The range is 1 to 2,147,483,647. The default is 10 seconds.

3 Configuration Examples

The following sections provide AAA configuration examples.

3.1 Configure Administrator Authentication

The following example shows how to enable local administrator authentication using remote console access, and limiting the number of concurrent sessions to 10:

```
[local]Redback(config-ctx)#aaa authentication administrator vty local maximum sessions 10
```

3.2 Configuration Administrator Accounting

The following example shows how to enable RADIUS accounting messages for administrator sessions for the local context:

```
[local]Redback(config-ctx)#aaa accounting administrator radius
```

3.3 Define the Administrator Structured Username

The following example shows how to define the username. In this case, the chassis checks for the far right separator, and an @ symbol.

```
[local]Redback(config-ctx)#aaa username-format domain @ rightmost-separator
```

3.4 Subscriber Authentication

You can configure subscriber authentication in several different ways. For example, different subscribers can be authenticated by different RADIUS servers in distinct contexts.

In the following example, subscriber **janet** in the **AAA_local** context is authenticated by the configuration in that context; subscriber **rene** in the **AAA_radius** context is authenticated by the RADIUS server in that context; and subscriber **kevin** in the **AAA_global** context is authenticated by the RADIUS server in the **local** context:

```
[local]Redback(config)#aaa global authentication subscriber radius context local
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius server 10.1.1.1 key TopSecret
.
.
.
[local]Redback(config)#context AAA_local
[local]Redback(config-ctx)#aaa authentication subscriber local
[local]Redback(config-ctx)#interface corpA multibind
[local]Redback(config-if)#ip address 10.1.3.30 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#subscriber name janet
[local]Redback(config-sub)#password dragon
[local]Redback(config-sub)#ip address 10.1.3.30 255.255.255.0
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 1 100 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber janet@AAA_local password dragon
.
.
.
[local]Redback(config)#context AAA_radius
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#radius server 10.2.2.2 key TopSecret
[local]Redback(config-ctx)#interface corpB multibind
[local]Redback(config-if)#ip address 10.2.4.40 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 2 200 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber rene@AAA_radius password tiger
.
.
.
[local]Redback(config)#context AAA_global
[local]Redback(config-ctx)#aaa authentication subscriber global
[local]Redback(config-ctx)#interface corpC multibind
[local]Redback(config-if)#ip address 10.3.5.50 255.255.255.0
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 6/1
[local]Redback(config-atm-oc)#atm pvc 3 300 profile ubr encapsulation bridge1483
[local]Redback(config-atm-pvc)#bind subscriber kevin@AAA_global password lion
```

3.5 Subscriber Reauthorization

The following example enables RADIUS reauthorization for subscriber circuits and accounting messages:

```
[local]Redback(config-ctx)#radius server 10.10.11.12 key redback
[local]Redback(config-ctx)#radius attribute nas-ip-address interface loop1
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#aaa accounting subscriber radius
[local]Redback(config-ctx)#aaa accounting reauthorization subscriber radius
[local]Redback(config-ctx)#aaa update subscriber 10
[local]Redback(config-ctx)#aaa accounting event reauthorization
[local]Redback(config-ctx)#aaa reauthorization bulk radius
[local]Redback(config-ctx)#radius accounting server 10.10.11.2. key redback
```