ERICSSON

Configuring RADIUS

SYSTEM ADMINISTRATOR GUIDE

65/1543-CRA 119 1170/1-V1 Uen H

Contents

1 Overview

This document provides an overview of Remote Authentication Dial-In User Service (RADIUS) support on the SmartEdge router and describes the tasks used to configure, monitor, and administer RADIUS features. This document also provides examples of configurations for RADIUS features.

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.

The RADIUS protocol, which is based on a client/server architecture, enables remote access to networks and network services. When configured with the IP address or hostname of a RADIUS server, the SmartEdge router can act as a RADIUS client.

To enable authentication through RADIUS, you must also configure authentication, authorization, and accounting (AAA) features; for more information, see *Configuring Authentication, Authorization, and Accounting*. Since some subscribers may be running IPv6, if you need information on IPv6, refer to *Configuring IPv6 Subscriber Services*.

1.1 RADIUS Servers

RADIUS servers can perform the following functions:

- Accounting server—Maintains accounting records for subscribers. The SmartEdge router transmits session start and stop times in Accounting Start and Stop messages to the server. Accounting is the process of tracking activity and network resources used in a subscriber session, including the number of packets and bytes transmitted during the session. It occurs after the authentication phase in AAA is complete. Accounting can occur for specific contexts, enabling customers to manage activity in their individual accounts. In addition, AAA accounting enables you to track the services used by an Internet site owner. When you enable AAA accounting, the router reports user activity to the RADIUS server in the form of accounting records. Common services tracked through service accounting include voice and video.

- Authentication server—Maintains authentication records for subscribers. The SmartEdge router requests authentication in Access Request messages before permitting subscribers access.

  A RADIUS server can also act as a Change of Authorization (CoA) server, allowing dynamic RADIUS-guided services for subscriber sessions. You can configure up to 36 CoA servers per context (optionally in redundant mode), to control BRAS functions by enabling and disabling RSE services and disconnecting sessions to resolve issues.

  The SmartEdge router supports both RADIUS CoA messages and disconnect messages. CoA messages can modify the characteristics of existing subscriber sessions without loss of service; disconnect messages can terminate subscriber sessions. Throughout this document, the term *RADIUS server* refers to any of the server types. The terms *RADIUS accounting server*, *RADIUS authentication server*, and *RADIUS CoA server* refer to servers that support those specific features.

- Accounting and authentication—Performs the functions of both the accounting and authentication servers.

For more information about RADIUS messages, see *RADIUS Attributes*.

Load balancing between multiple servers is valuable if a large number of sessions are established and terminated every second, and a single RADIUS server is unable to handle the load.

Two load-balancing algorithms are supported:

- Strict-priority—Requests are always sent first to the first server configured in the SmartEdge router. If the request fails, the requests are sent to the next server and so on.

- Round-robin priority—Requests are sent to the server following the one where the last request was sent. If the SmartEdge router receives no response from the server, requests are sent to the next server and so on.

1.2 RADIUS Service Engine Features

The RADIUS Service Engine (RSE) is the set of RADIUS-guided features and functions that support dynamic changes to subscriber services.

RADIUS-guided services include the following:

- RADIUS-guided HTTP redirect—See *Configuring HTTP Redirect*

- Dynamic ACLs—See *Configuring ACLs*

- RADIUS-guided forward policies—See *Configuring Forward Policies*

- RADIUS-guided NAT policies (attached to received traffic only)—See *Configuring NAT Policies*
- RADIUS-guided QoS metering and policing policies—See *Configuring Rate-Limiting and Class-Limiting*
- Dynamic changes to QoS metering, policing, and PWFQ policy options—See *Configuring Rate-Limiting and Class-Limiting* and *Configuring Queuing and Scheduling*

To support RADIUS-guided services, the SmartEdge router uses a service profile that specifies various service conditions and that activates services and establishes the service conditions for that subscriber session. It is these service conditions against which the service data in a CoA Request or Access Response message is matched.

A service condition in a RADIUS-guided service profile can be mandatory or optional. For a mandatory condition, the RADIUS server must include a value for that condition in the CoA Request or Access Response message. An optional condition includes a default value in the service profile; the SmartEdge router uses default value if the RADIUS server does not supply a value.

1.3 Accounting and Service Accounting Messages

In addition to providing authentication, a RADIUS server collects and stores accounting data for subscriber sessions. Accounting is the process of tracking activity and network resources used in a subscriber session. The process tracks the number of packets and bytes transmitted during the session. It occurs after the authentication phase. Accounting can occur for specific contexts, enabling customers to manage activity in their individual accounts.

The AAA accounting feature also enables you to track the services used by an Internet site, for example, a wholesaler. The SmartEdge router reports service activity to the RADIUS server in the form of accounting records. Common services tracked through service accounting are voice and video.

As part of both general accounting and service accounting, the router generates messages indicating the states of the accounting process. Common service messages indicate when the router starts and stops sending service accounting packets to the RADIUS server. For example, when the router initiates accounting, the router generates a message (with an acct-start message) indicating the accounting process has begun.

While accounting messages can be helpful to identify accounting states, they create overhead, using system memory and CPU resources. To manage overhead associated with this activity, the operating system enables you to configure the SmartEdge router to drop RADIUS accounting messages in a specific context. To drop a message, you specify the message using the **`attribute`** command.

Common service messages indicate when the router begins and stops sending service accounting packets to the RADIUS server. The router sends these packets to the server when the RADIUS Change of Authorization (CoA) server initiates these actions.

For general accounting, the router generates the following messages:

- access-request—Indicates a client-generated Access-Request message that includes a login and a password.
- acct-start—An Accounting-Request message that indicates an accounting process has started.
- acct-stop—An Accounting-Request message that indicates an accounting process has stopped.
- acct-on—An Accounting-Request message that indicates an accounting process has been enabled.
- acct-off—An Accounting-Request message that indicates an accounting process has been disabled.
- acct-update— An Accounting-Request message which includes updates, such as tracking and reporting the number of packets and bytes transmitted during a subscriber session.

For service accounting, the router generates the following messages:

- service-acct-update—Indicates that a service accounting process has entered the interim stage.
- service-acct-start—Indicates that a service accounting process has stopped.
- service-acct-stop—Indicates that a service accounting process has started.

Figure 1 shows the flow of service accounting messages.

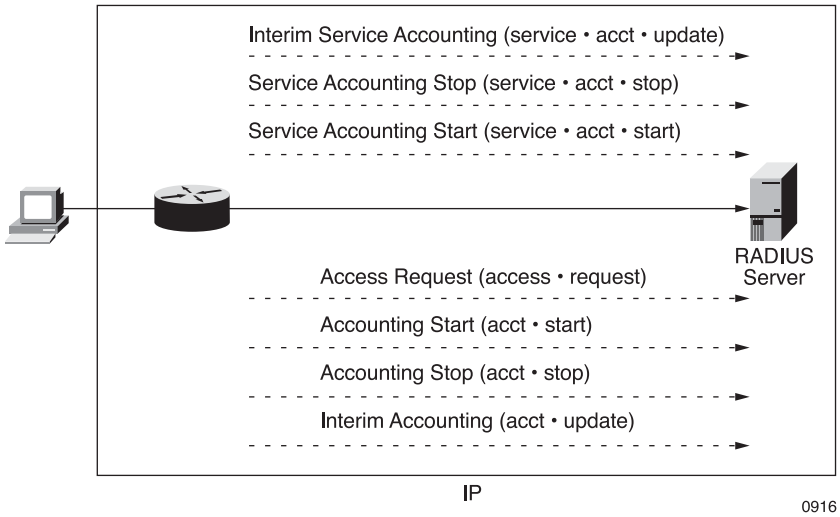

Figure 1 Flow of Service Accounting Messages

2 Configuration and Operations Tasks

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

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

2.1 Configuring the Server IP Address or Hostname

To configure the IP address or hostname of a RADIUS accounting server or RADIUS server, perform the appropriate task described in Table 1. Enter all commands in context configuration mode.

Table 1 Configure the Server IP Address or Hostname

Task	Root Command	Notes
Configure the RADIUS accounting server IP address or hostname.	*radius accounting server*	To enable accounting through RADIUS, you must also enter the **`aaa accounting subscriber radius`** command (in context configuration mode).
Configure the RADIUS server IP address or hostname.	*radius server*	To enable authentication through RADIUS, you must also enter the **`aaa authentication subscriber radius`** command (in context configuration mode). To use the RADIUS server as a CoA server, use the **`CoA-server`** keyword for this command. To configure an independent CoA server, use the *radius coa server* command.
Configure the RADIUS server as a CoA server.	*radius coa server*	You can configure up to 36 CoA servers per context. To configure independent CoA servers, enter this command one or more times. To use the RADIUS authentication server as a CoA server, use the **`CoA-server`** keyword with the *radius server* command.

2.2 Configuring an IP Source Address (Optional)

By default, the local IP address of the interface on which RADIUS is transmitted is included in the IP header of RADIUS packets sent by the SmartEdge router. If you do not want to publish the IP address of the RADIUS server, configure a loopback interface to appear to be the source address for RADIUS packets as described in Table 2.

Table 2 Configure an IP Source Address

Task	Root Command	Notes
Configure an IP source address.	*ip source-address radius*	Enter this command in interface configuration mode. The interface must be reachable by the RADIUS server; for command details, see *Configuring Contexts and Interfaces*.

2.3 Configuring Load Balancing Between RADIUS Servers (Optional)

To load balance between multiple RADIUS accounting or RADIUS servers, perform the appropriate task described in Table 3. Enter all commands in context configuration mode.

Table 3 Configure Load Balancing Between RADIUS Servers

Task	Root Command
Specify a load-balancing algorithm to use among multiple RADIUS accounting servers.	*radius accounting algorithm*
Specify a load-balancing algorithm to use among multiple RADIUS servers.	*radius algorithm*

2.4 Modifying RADIUS Connection Parameters (Optional)

To configure how the SmartEdge router responds to connections with RADIUS servers, perform the tasks described in the following sections.

2.4.1 Send Accounting On and Off Messages

To send Accounting On or Accounting Off messages to any other RADIUS servers that are configured in the current context when a RADIUS server is added or removed, perform the task described in Table 4.

Table 4 Send Accounting On and Off Messages

Task	Root Command	Notes
When an accounting server is added to or removed from the configuration, send an accounting on or accounting off message, respectively, to any other RADIUS servers that are configured in the current context.	*radius accounting sendacctonoff*	Enter this command in context configuration mode. By default, the SmartEdge router sends these messages.

2.4.2 Modifying RADIUS Time-out Parameters

RADIUS time-out parameters allow you to configure three different intervals used by the system to manage responses when a RADIUS server is not responding. Table 5 describes the intervals and how you can configure them. When determining whether a RADIUS sever should be marked "dead," the SmartEdge router defines the time at which the last successful response was received from the server as time T0.

Table 5 RADIUS Time-out Intervals

Time	RADIUS Action	Interval Set By
T0	The time that the last successful response was received from the RADIUS server. Timer set for interval T2. This is the interval in which the SmartEdge router expects a response from the RADIUS server.	**radius server-timeout** **radius accounting server-timeout**
T*x*	Time at which the SmartEdge router sends a request to the RADIUS server. Timer set for interval T1.	**radius timeout**
T*x*+T1	If no response, the SmartEdge router assumes that the packet is lost or the server is unreachable. T1 expires.	**radius server-timeout** **radius accounting server-timeout**
T0+T2	T2 expires. If T*x* is greater than T0+T2, the SmartEdge router marks the server as “dead” and tries another server. Timer set for interval T3.	**radius deadtime** **radius accounting deadtime**
T0+T2+T3	T3 expires. The SmartEdge router sends another request to the first server.	–

To modify the RADIUS time-out parameters that the SmartEdge router uses for managing the connections to and from RADIUS servers and RADIUS accounting servers, perform the appropriate tasks described in Table 6. Enter all commands in context configuration mode.

Table 6 Modify RADIUS Time-out Parameters

Step	Task	Root Command	Notes
1.	Optional. Modify the interval that the SmartEdge router waits for a response from a RADIUS server after sending a packet:		
	For a RADIUS accounting server	*radius accounting timeout*	
	For a RADIUS server	*radius timeout*	
2.	Optional. Modify the maximum number of retransmission attempts during the time-out interval:		
	For a RADIUS accounting server	*radius accounting maxretries*	
	For a RADIUS server	*radius maxretries*	
3.	Optional. Modify the interval that the SmartEdge router waits for a response before marking a nonresponsive server “dead”:		
4.	For a RADIUS accounting server	*radius accounting servertimeout*	Setting the value to 0 disables the feature.
5.	For a RADIUS server	*radius servertimeout*	
6.	Optional. Modify the interval that the SmartEdge router treats a nonresponsive server as “dead” before trying to reach it again:		
	For a RADIUS accounting server	*radius accounting deadtime*	Setting this value to 0 disables the feature.
	For a RADIUS server	*radius deadtime*	
7.	Optional. Modify the number of outstanding requests that can be sent:		

Table 6 Modify RADIUS Time-out Parameters

Step	Task	Root Command	Notes
	For a RADIUS accounting server.	*radius accounting maxoutstanding*	
	For a RADIUS server	*radius accounting maxoutstanding*	

2.5 Stripping the Domain Portion of Structured Usernames (Optional)

To specify that the domain portion of structured usernames is to be removed before sending the usernames to a RADIUS server for authentication, perform the task described in Table 7.

Table 7 Strip the Domain Portion of Structured Usernames

Task	Root Command	Notes
Strip the domain portion of structured usernames.	*radius stripdomain*	Enter this command in context configuration mode.

2.6 Changing or Ignoring the Server Source Port Value (Optional)

To increase the number of outstanding authentication requests per RADIUS server by sending the requests, using a different source port value, perform the task described in Table 8.

Table 8 Change the Server Source Port Value

Task	Root Command	Notes
Change the server source port value.	*radius sourceport*	Enter this command in global configuration mode.

To enable the SmartEdge router to ignore the source port sent by a RADIUS server in an Access-Response message, perform the task described in Table 9.

Table 9 Ignore the Server Source Port Value

Task	Root Command	Notes
Ignore the server source port value in RADIUS Access-Response messages.	*radius sourceport*	Enter this command in context configuration mode.

2.7 Configuring and Assigning a RADIUS Policy to a Context (Optional)

A RADIUS policy specifies which RADIUS attributes and vendor-specific attributes (VSAs) are to be removed from RADIUS Access-Request, Access-Accept, CoA, and various Accounting-Request messages (Accounting-On, Accounting-Off, Accounting-Start, Accounting-Stop, and Accounting-Update). Up to 30 policy filters can be defined. To configure and assign a RADIUS policy to a context, perform the tasks described in Table 10.

Table 10 Configure and Assign a RADIUS Policy to a Context

Step	Task	Root Command	Notes
1.	Create or modify a RADIUS policy and access RADIUS policy configuration mode.	*radius policy*	Enter this command in global configuration mode.
2.	Specify the RADIUS Attribute or VSA to be sent in Access-Request or Accounting-Request messages. Optionally, using configuration, indicate whether an attribute or a VSA should be dropped. In the absence of any configuration, all messages containing RADIUS attributes or VSAs will be sent; no messages will be dropped.	*attribute*	Enter this command in RADIUS policy configuration mode.
3.	Assign the policy to a context.	*radius policy*	Enter this command in context configuration mode.

2.8 Configuring and Sending Attributes in RADIUS Packets (Optional)

To configure and send attributes in RADIUS request packets, perform one or more of the tasks described in Table 11. Enter all commands in context configuration mode, unless otherwise indicated.

Table 11 Configure and Send Attributes in RADIUS Request Packets

Task	Root Command	Notes
Send the Acct-Delay-Time attribute in RADIUS Access-Request and Accounting-Request packets.	*radius attribute acctdelaytime*	By default, this attribute is not sent.
Send the Acct-Session-Id attribute in RADIUS Access-Request packets.	*radius attribute acctsessionid*	By default, this attribute is sent only in Accounting-Request packets.
Send a Layer 2 Tunneling Protocol (L2TP) call serial number type value in the Acct-Tunnel-Connection attribute in RADIUS packets.	*radius attribute accttunnelconnection l2tp-call-serial-num*	By default, this attribute is not sent.
Specify the behavior of the SmartEdge router when it receives a RADIUS Filter-Id attribute that does not specify a direction and there is an access control list (ACL) applied to the circuit.	*radius attribute filter-id*	By default, this attribute is not sent.
Send the NAS-Identifier attribute in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasidentifier*	By default, this attribute is not sent.
Send the NAS-IP-Address attribute for IPv4 subscribers in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasipaddress*	By default, this attribute is not sent.
Send the NAS-IPv6-Address attribute for IPv6 subscribers in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasipv6address*	By default, this attribute is not sent.
Modify the format in which the NAS-Port attribute is sent in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasport*	By default, this attribute is sent using the **`slot-port`** format.

Table 11 Configure and Send Attributes in RADIUS Request Packets

Task	Root Command	Notes
Modify the format in which the NAS-Port-Id attribute in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasportid*	By default, this attribute is sent using the `all` format.

Table 11 Configure and Send Attributes in RADIUS Request Packets

Task	Root Command	Notes
Modify the value of the NAS-Port-Type attribute sent in RADIUS Access-Request and Accounting-Request packets.	*radius attribute nasporttype*	Enter this command in ATM profile, dot1q profile, link group, or port configuration mode. By default, this attribute is sent using a value of either 0 or 5, indicating an asynchronous connection through a console port or a virtual connection through a transport protocol, respectively. **Note:** For link groups, the NAS-Port-Type attribute can be set only at the link-group level, not for the constituent ports. Any ports that already have the NAS-Port-Type attribute configured cannot be added to a link group until this configuration is removed from the port.
Specify the character the SmartEdge router uses to separate the fields for the medium access control (MAC) addresses in the vendor VSA 145 provided by Ericsson AB, Mac-Addr, specify whether attributes can be encrypted, or specify whether to enable IPv4 address save mode for the context in the vendor VSA 213 provided by Ericsson AB, IPv4-Address-Release-Control.	*radius attribute vendorspecific*	By default, the MAC address separator is hyphen (-), vendor VSAs can be encrypted, and IPv4 address save mode is disabled.

2.8.1 RADIUS Support for IPv6 Subscriber Services

For 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)
- Delegated-IPv6-Prefix (123)
- RB-IPv6-DNS (207)
- RB-IPv6-Option (208)

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

2.9 Configuring RADIUS-Guided Services (Optional)

To enable RADIUS-guided services for subscriber sessions using a service profile, and to configure how the SmartEdge router responds to connections with RADIUS servers, perform the tasks described in the following sections.

2.9.1 Configuring the RADIUS-Guided Policies for the Service Profile

Configure one or more RADIUS-guided policies, such as a forward policy, NAT policy, or QoS metering or policing policy, to be applied to the subscriber record or profile. For more information, see *Configuring Forward Policies*, *Configuring NAT Policies*, and *Configuring Rate-Limiting and Class-Limiting*.

2.9.2 Configuring a RADIUS-Guided Service Profile

Configure the service profile that references the RADIUS-guided policies that you have configured. To configure a RADIUS-guided service profile, perform the tasks in Table 12; enter all commands in service profile configuration mode, unless otherwise indicated.

Table 12 Configure a RADIUS-Guided Service Profile

Step	Task	Root Command	Notes
1.	Create or select a context in which to configure the policies and service profile and access context configuration mode.	*context*	Enter this command in global configuration mode.
2.	Create or select the service profile and access service profile configuration mode.	*radius service profile*	Enter this command in context configuration mode.
	Specify a service condition for the service profile and its default condition, if necessary.	*parameter*	Enter this command to specify a mandatory or optional condition for the profile.
	Optional. Specify counters for service accounting.	*accounting*	
	Specify a service policy attribute with its options.	*attribute*	Enter this command to specify an attribute for each service condition in this profile.
	Specify a parameter that can have multiple values.	*foreach*	Enter this command preceding an **`attribute`** command when a field has multiple values.

2.9.3 Configuring the Subscriber Profile or Record

Configure the subscriber profile or record. You do not apply the policies to the subscriber profile or record; they are specified by the RADIUS server and applied by the RADIUS-guided service profile.

2.10 RADIUS Service Engine

RSE provides a framework to activate and deactivate subscriber services dynamically. You can use the RSE framework for various applications or subscriber services. The service volume limits per direction and Service Absolute timer limits can be reauthorized. RSE supports reauthorization of the service parameters or attributes dynamically when the service is active. However, not all service parameters can be reauthorized.

The following example outlines the steps in a typical service reauthorization scenario—in this case, for VoIP:

1. The subscriber attempts to connect to router.

2. The connection attempt triggers authentication of the subscriber towards the RADIUS server using an Access-Request.
3. The RADIUS server validates the response and, upon success, responds back with Access-Accept along with the services the user subscribes to—VoIP service, with a default service time-out of 600 seconds.
4. Access is granted, and the VoIP service is enabled.
5. If the user subscribes to a premium VoIP service, the RADIUS server sends a COA-Request for the existing VoIP service, with a new service time-out of 1200 seconds.
6. On successful provision, the router responds back with a COA-Response (indicating success), and the service time-out for the VoIP service is increased to 1200 seconds.

2.11 Configuring Service Absolute Time-out Values

To configure the service absolute time-out value, enter commands in the RADIUS service profile mode.

The following example shows how to configure the time-out value. The context name is `RSE`, and the router name is `router`:

```
[RSE]router#config
Enter configuration commands, one per line, 'end' to exit
[RSE]router(config)#context RSE
[RSE]router(config-ctx)#radius service profile HTTP-REDIR
[RSE]router(config-service-profile)#service-action absolute-timeout acct-alive
<cr>
```

The service time-out value is an absolute time of the service since the service started. If the service time is greater than or equal to the new time-out value, the service is deactivated immediately. However, the service is not deactivated if the **`service action`** command is configured. The current timer is restarted at AAA with new value, and the change takes effect immediately.

When the **`absolute-timeout service action`** command is configured, and the service absolute timer has been reached, the RADIUS server receives a Service-Alive accounting message; however, the service is not deactivated.

The valid range for the time-out value is from 1 to 2147483647 seconds. If the absolute time-out service action is set, a Service-Alive accounting packet is sent to the RADIUS server.

If the service action is not set, the service remains deactivated.

2.12 Verifying the Service Absolute Time-out Values

Use the **`show configuration`** command to verify that you have configured the absolute time-out values:

```
[RSE]router#show configuration
Building configuration...

Current Configuration:

!
 radius service profile HTTP-REDIR
  service-action absolute-timeout acct-alive
  parameter value prof
  parameter value url
  parameter value svc-timeout
  parameter value in-limit
  accounting in fwd PASSTHRU
  seq 10 attribute HTTP-Redirect-Profile $prof
  seq 20 attribute Forward-Policy in http_redir_policy
  seq 30 attribute Service-Interim-Accounting 900
  seq 40 attribute Service-Timeout $svc-timeout
  seq 50 attribute HTTP-Redirect-url $url
  seq 60 attribute Service-Volume-Limit in $in-limit
```

2.13 Configuring the Service Traffic Limit

In the RADIUS service profile, you can configure the service action traffic limit by using the **service-action traffic-limit acct-alive** command:

```
[RSE]router(config-ctx)#radius service profile HTTP-REDIR

[RSE]router(config-service-profile)#service-action traffic-limit
acct-alive
```

When the **service-action traffic-limit acct-alive** command is configured, and the service action traffic limit has been reached, you receive a Service-Alive accounting message; however, the service is not deactivated.

If the service-action traffic limit is not set, the service remains deactivated.

2.14 Verifying the Configured Service Traffic Limit

Use the **show configuration** command to verify that you have configured the service traffic limit:

```
[RSE]Redback#show configuration
Building configuration...

Current configuration:
!
 radius service profile HTTP-REDIR
  service-action traffic-limit acct-alive
  parameter value prof
  parameter value url
  parameter value svc-timeout
  parameter value in-limit
  accounting in fwd PASSTHRU
  seq 10 attribute HTTP-Redirect-Profile $prof
  seq 20 attribute Forward-Policy in http_redir_policy
  seq 30 attribute Service-Interim-Accounting 900
  seq 40 attribute Service-Timeout $svc-timeout
  seq 50 attribute HTTP-Redirect-url $url
  seq 60 attribute Service-Volume-Limit in $in-limit
```

2.15 RADIUS-Guided Service Audit for Volume Counters

You can send SNMP queries using the RBN-SUBSCRIBER-ACTIVE-MIB to retrieve a snapshot of each subscriber's RADIUS-guided service volume counters while a volume-limit-enabled subscriber session is active.

2.16 Configuring and Overwriting the NAS-Port-Id RADIUS Attribute

On Ethernet and ATM cards, you can configure and overwrite the NAS-Port-Id RADIUS attribute. NAS-Port-ID indicates the physical slot/port number of the NAS that is authenticating the user. Configure the NAS-Port-Id by using the **radius attribute nas-port-id** ***slot/port*** command at the port level command mode. You can configure command on multiple ports.

When configuring or unconfiguring the slot/port values using the CLI after a session is successfully created, it will not have any effect on the NAS-Port-Id of the existing session. However, the NAS-Port-Id attribute of all the subsequently created sessions will have the following impact:

- When configuring the CLI, the NAS-Port-Id is overwritten with the new slot/port values.
- When unconfiguring the CLI, the NAS-Port-Id will revert back to receiving the slot/port information from the circuit.

The NAS-Port-Id overwrite function is restricted to PPPoE/PPPoEoA-based subscribers. Configuring the **radius attribute nas-port-id x/y** command has no effect on non-PPPoE subscribers. When configured at the port level, slot/port substitution is performed for all circuits configured under that port, and has no impact on link-group subscribers.

- When you configure the slot/port values of a redundant chassis using the **radius attribute nas-port-id** CLI command, these values represent the slot/port of the redundant chassis.

2.16.1 Enabling Overwriting the NAS-Port-Id RADIUS Attribute

To enable overwriting of the NAS-Port-ID, use the following command syntax:

```
[local]Redback(config-port)# radius attribute nas-port-id slot/port
```

- ***slot***: 1 – 14 (Maximum value varies by platform.)
- ***port***: 1 – 64 (The maximum number of ports per card supported by SmartEdge router chassis is 64.)

If you configure a slot value outside the valid ranges, the following error message will be displayed to prevent slot misconfiguration:

```
[local]Redback(config-port)#radius attribute nas-port-id 99/1
                                                         ^
% Invalid input at '^' marker
```

To correct this error, specify a slot value between 1-14.

Similarly, if you configure a port value outside the valid ranges, the following error message will be displayed to prevent port misconfiguration:

```
[local]Redback(config-port)#radius attribute nas-port-id 14/65
                                                          ^
% Invalid input at '^' marker
```

Again, to correct this error, specify a port value between 1-64.

2.16.2 Disabling Overwriting the RADIUS Attribute

```
[local]Redback(config)#port ethernet slotX/portY
[local]Redback(config-port)#no radius attribute nas-port-id
```

To disable overwriting the RADIUS attribute, enter the following commands at the port configuration level:

```
[local]Redback(config)#port ethernet slotX/portY
[local]Redback(config-port)#no radius attribute nas-port-id
```

2.17 Verifying Slot or Port Configuration

When NAS-Port-Id is not configured or has been unconfigured, the **show configuration** command displays the following information:

```
Current configuration:
port ethernet <slotA/slotB>
 no radius attribute nas-port-id
!
```

When you have correctly configured your slot/port values, to ensure that you have overwritten the NAS-Port-Id, and to view the existing NAS Port Type command under the port level, use the **show port** *slot/port* **detail** command. When these attributes are not configured, no values are displayed.

The following example shows the information displayed by the **show port** *slot/port***detail** command:

```
[local]Redback#show port 5/1 detail

ethernet 5/1 state is No card
Description                 :
Line state                  : No card
Admin state                 : Down
Link Dampening              : disabled
Undampened line state       : No card
Dampening Count             : 0
Encapsulation               : ethernet
MTU size                    : 1500 Bytes
NAS Port Type               : 4
NAS-Port-ID                 : 3/4
Media type                  : Unknown

Auto-negotiation            : on                  state: unknown
   Flc negotiated set       : tx&rx-or-rx-only    state: unknown
   force                    : disabled            state: inactive
Flow control                : rx                  state: n/a
Link Distance               : N/A
Loopback                    : off
Active Alarms               : N/A
```

2.18 Remapping Account Termination Codes (Optional)

When a subscriber session is terminated, the system reports the reason for the termination to RADIUS, using one of several terminate cause codes that are defined in RFC 2866, `RADIUS Accounting`, in attribute 49 (Acct-Terminate-Cause). Because the set of codes defined for RADIUS attribute 49 is very limited, the SmartEdge router defines a more extensive set of terminate cause codes to more precisely indicate the reason for the termination. The system transmits these codes in vendor VSA 142 (Session-Error-Code) and 143 (Session-Error-message).

Terminate error codes and their RADIUS attribute 49 error codes are listed in the RADIUS Attribute 49 Error Codes section in *RADIUS Attributes*. You can change the RADIUS attribute 49 error code for a Redback terminate cause code to a different attribute 49 error code.

To remap an Redback terminate error code to a different RADIUS attribute 49 error code, perform the tasks described in Table 13.

Table 13 Remap Redback Terminate Error Codes

Task	Root Command	Notes
Enable the remapping of account termination error codes and access terminate error cause configuration mode.	*radius attribute acctterminatecause remap*	Enter this command in global configuration mode.
Remap a Redback terminate error code to a different RADIUS attribute 49 error code.	*rbaktermec*	Enter this command in terminate error cause configuration mode for each Redback terminate error code that you want to remap.

2.19 Operations Tasks

To monitor, troubleshoot, and administer RADIUS features, perform the RADIUS operations tasks described in Table 14. Enter the **`clear`** and **`debug`** commands in exec mode; enter the **`show`** commands in any mode.

Table 14 RADIUS Operations Tasks

Task	Root Command
Clear RADIUS counters for access and accounting messages.	*clear radius counters*
Enable the generation of RADIUS debug messages.	*debug radius*
Display RADIUS server control information.	*show radius control*
Display RADIUS access, accounting, and CoA message counters.	*show radius counters*
Display RADIUS server configuration and status information, including accounting, authentication, and CoA servers.	*show radius server*
Display RADIUS server statistics about accounting, authentication, and CoA servers.	*show radius statistics*
Display RADIUS CoA server configuration.	*show configuration | grep coa*
Verify RSE configuration.	*show subscriber active agent-circuit-id cct-id* *show access-group subscriber sub-name@ctx-name [detail]*

3 Configuration Examples

This section provides examples of configuring RADIUS secret key, retry, and time-out settings, a RADIUS loopback interface, a custom RADIUS policy, and a dynamic RADIUS profile and forward policy.

3.1 RADIUS Secret Key, Retry, and Time-out

The following example shows how to configure the IP address of the RADIUS server, **10.43.32.56**, using the key, **Secret**, and configure related behaviors of the SmartEdge router:

```
[local]Redback(config-ctx)#radius server 10.43.32.56 key Secret
[local]Redback(config-ctx)#radius max-retries 5
[local]Redback(config-ctx)#radius timeout 30
```

3.2 RADIUS Loopback Interface

The following example configures the interface at IP address, **108.1.1.1**, to connect to the RADIUS server; however, a loopback interface is also configured using IP address, **11.200.1.1**, which is sent to the RADIUS server as the source IP address for RADIUS packets.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to-radius-server
[local]Redback(config-if)#ip address 108.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface loop1 loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#ip source-address radius
```

3.3 Custom RADIUS Policy

The following example creates the **custom** RADIUS policy to drop RADIUS attribute **123** in all RADIUS messages, vendor VSA **10** in Access-Request messages, and vendor VSAs **11** and **12** in various Accounting messages, and then assigns it to the **gold-isp** context:

```
[local]Redback(config)#radius policy name custom
[local]Redback(config-rad-policy)#attribute 123 drop
[local]Redback(config-rad-policy)#attribute rbak 10 drop access-request
[local]Redback(config-rad-policy)#attribute rbak 11 drop acct-start acct-update
[local]Redback(config-rad-policy)#attribute rbak 12 drop acct-start acct-stop
[local]Redback(config-rad-policy)#exit
[local]Redback(config)#context gold-isp
[local]Redback(config-ctx)#radius policy custom
```

3.4 Dynamic RADIUS Profile and Forward Policy

The following examples create a RADIUS-guided forward policy and a RADIUS-guided service profile that specifies the dynamic service conditions for the forward policy. After the initial configuration in global mode, subsequent configurations are created in the **local** context as shown in the example. The subscriber configuration on a RADIUS server is listed after the service profile.

First, in global mode, you create a RADIUS-guided forward policy with three classes. The forward policy redirects one class with an ACL policy and takes no action on the other two classes. For the class named **portal** you set the optional field name for the destination port number for the portal class to 80 and the service time-out value to **900**.

```
[local]Redback(config)#forward policy captive-portal radius-guided
[local]Redback(config-policy-frwd)#access-group
[local]Redback(config-policy-group)#class redirect
[local]Redback(config-policy-group-class)#redirect destination local
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class portal
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class bypass
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-frwd)#exit
```

Create a service profile for the redirect and portal classes of traffic:

```
[local]Redback(config-ctx)#radius service profile redirect
```

Specify the URL field name for the redirect class:

```
[local]Redback(config-svc-profile)#parameter value redirect-url
```

Specify the field name for the IP address of the destination port for the portal class:

```
[local]Redback(config-svc-profile)#parameter value portal-ip
[local]Redback(config-svc-profile)#parameter value portal-port 80
```

Specify the field name for an array of TCP port numbers for the redirect class:

```
[local]Redback(config-svc-profile)#parameter list tcp-port
[local]Redback(config-svc-profile)#parameter value service-timeout 900
```

Enable accounting for incoming traffic for the redirect class:

```
[local]Redback(config-svc-profile)#accounting in fwd redirect
```

Specify the fields in the attributes for dynamic service conditions. Names beginning with $ are replaced when the value of the field is specified by a RADIUS server. Names are those previously defined by the parameter statements. Specify the name of the forward policy; in this example, all subscriber sessions use the same policy:

```
[local]Redback(config-svc-profile)#attribute Forward-Policy "in:$captive-portal"
```

Specify the field name for the dynamic URL for the redirect class:

```
[local]Redback(config-svc-profile)#attribute HTTP-Redirect "$redirect-url"
```

Specify the field name for the service time-out:

```
[local]Redback(config-svc-profile)#attribute Service-Timeout "$service-timeout"
```

Specify the field names for the IP address and port number for the portal class:

```
[local]Redback(config-svc-profile)#attribute Dynamic-Policy-Filter "ip in forward dstip
$portal-ip tcp dstport = $portal-port class portal fwd"
```

Specify the TCP port array for the destination port numbers for the redirect class:

```
[local]Redback(config-svc-profile)#foreach tcp-port
[local]Redback(config-svc-profile)#attribute Dynamic-Policy-Filter "ip in forward tcp
 dstport = $tcp-port class redirect fwd"
```

RADIUS server subscriber configuration with values for the dynamic service conditions. In this example, the dynamic conditions are tagged with the value 1. Specify the name of the service profile:

```
Redback-Service-Name:1 = "redirect"
```

Enable service accounting:

```
Redback-Service-Options:1 = 0x01
```

Specify the service condition field names. Specify the redirect URL:

```
Redback-Service-Parameters:1 = "redirect-url=http://172.16.1.1/portal.php"
```

Specify the destination IP address for the portal class. Use the default value in the profile for the port number:

```
Redback-Service-Parameters:1 = "portal-ip=172.16.1.1/32"
```

Specify the TCP port numbers for the redirect class:

```
Redback-Service-Parameters:1 = "tcp-port=www,443,8080"
```

Specify the time-out interval; this value overrides the default value (900):

```
Redback-Service-Parameters:1 = "Service-Timeout=1800"
```

3.5 NAS IPv6 Address

The following example shows how to configure the NAS IPv6 address:

```
[local]BRAS#configure
[local]BRAS(config)#context SJ1
[local]BRAS(config-ctx)#radius attribute NAS-IPV6-Address interface if1
```

3.6 RADIUS CoA Servers

You can configure up to 36 CoA servers per context (optionally in redundant mode), to control BRAS functions by enabling and disabling RSE services and disconnecting sessions to resolve issues.

The following example shows the commands to configure 36 CoA servers in the local context:

```
[local]Redback(config-ctx)#radius coa server 1.1.1.1 encrypted-key 6840234DDC4A32D4 port 3799
[local]Redback(config-ctx)#radius coa server 1.1.1.2 encrypted-key 6840234DDC4A32D4 port 3800
[local]Redback(config-ctx)# radius coa server 1.1.1.3 encrypted-key 6840234DDC4A32D4 port 3801
[local]Redback(config-ctx)# radius coa server 1.1.1.4 encrypted-key 6840234DDC4A32D4 port 3802
[local]Redback(config-ctx)# radius coa server 1.1.1.5 encrypted-key 6840234DDC4A32D4 port 3803
[local]Redback(config-ctx)# radius coa server 1.1.1.6 encrypted-key 6840234DDC4A32D4 port 3804
[local]Redback(config-ctx)# radius coa server 1.1.1.7 encrypted-key 6840234DDC4A32D4 port 3805
[local]Redback(config-ctx)# radius coa server 1.1.1.8 encrypted-key 6840234DDC4A32D4 port 3806
[local]Redback(config-ctx)# radius coa server 1.1.1.9 encrypted-key 6840234DDC4A32D4 port 3807
[local]Redback(config-ctx)# radius coa server 1.1.1.10 encrypted-key 6840234DDC4A32D4 port 3808
[local]Redback(config-ctx)# radius coa server 1.1.1.11 encrypted-key 6840234DDC4A32D4 port 3809
[local]Redback(config-ctx)# radius coa server 1.1.1.12 encrypted-key 6840234DDC4A32D4 port 3810
[local]Redback(config-ctx)# radius coa server 1.1.1.13 encrypted-key 6840234DDC4A32D4 port 3811
[local]Redback(config-ctx)# radius coa server 1.1.1.14 encrypted-key 6840234DDC4A32D4 port 3812
[local]Redback(config-ctx)# radius coa server 1.1.1.15 encrypted-key 6840234DDC4A32D4 port 3813
[local]Redback(config-ctx)# radius coa server 1.1.1.16 encrypted-key 6840234DDC4A32D4 port 3814
[local]Redback(config-ctx)# radius coa server 1.1.1.17 encrypted-key 6840234DDC4A32D4 port 3815
[local]Redback(config-ctx)# radius coa server 1.1.1.18 encrypted-key 6840234DDC4A32D4 port 3816
[local]Redback(config-ctx)# radius coa server 1.1.1.19 encrypted-key 6840234DDC4A32D4 port 3817
[local]Redback(config-ctx)# radius coa server 1.1.1.20 encrypted-key 6840234DDC4A32D4 port 3818
[local]Redback(config-ctx)# radius coa server 1.1.1.21 encrypted-key 6840234DDC4A32D4 port 3819
[local]Redback(config-ctx)# radius coa server 1.1.1.22 encrypted-key 6840234DDC4A32D4 port 3820
[local]Redback(config-ctx)# radius coa server 1.1.1.23 encrypted-key 6840234DDC4A32D4 port 3821
[local]Redback(config-ctx)# radius coa server 1.1.1.24 encrypted-key 6840234DDC4A32D4 port 3822
[local]Redback(config-ctx)# radius coa server 1.1.1.25 encrypted-key 6840234DDC4A32D4 port 3823
[local]Redback(config-ctx)# radius coa server 1.1.1.26 encrypted-key 6840234DDC4A32D4 port 3824
[local]Redback(config-ctx)# radius coa server 1.1.1.27 encrypted-key 6840234DDC4A32D4 port 3825
[local]Redback(config-ctx)# radius coa server 1.1.1.28 encrypted-key 6840234DDC4A32D4 port 3826
[local]Redback(config-ctx)# radius coa server 1.1.1.29 encrypted-key 6840234DDC4A32D4 port 3827
[local]Redback(config-ctx)# radius coa server 1.1.1.30 encrypted-key 6840234DDC4A32D4 port 3828
[local]Redback(config-ctx)# radius coa server 1.1.1.31 encrypted-key 6840234DDC4A32D4 port 3829
[local]Redback(config-ctx)# radius coa server 1.1.1.32 encrypted-key 6840234DDC4A32D4 port 3830
[local]Redback(config-ctx)# radius coa server 1.1.1.33 encrypted-key 6840234DDC4A32D4 port 3831
[local]Redback(config-ctx)# radius coa server 1.1.1.34 encrypted-key 6840234DDC4A32D4 port 3832
[local]Redback(config-ctx)# radius coa server 1.1.1.35 encrypted-key 6840234DDC4A32D4 port 3833
[local]Redback(config-ctx)# radius coa server 1.1.1.36 encrypted-key 6840234DDC4A32D4 port 3834
```