ERICSSON

Commands: through al

COMMAND DESCRIPTION

Contents

1 Command Descriptions

Commands starting with numbers and symbols through commands starting with “al” are included.

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 ?

`?`

1.1.1 Purpose

Displays brief system help on the available commands or command options.

1.1.2 Command Mode

All modes

1.1.3 Syntax Description

This command has no keywords or arguments.

1.1.4 Default

None

1.1.5 Usage Guidelines

Use the **`?`** command to display brief system help on the available commands or command options.

To list all valid commands available in the current mode, enter a question mark (**?**) at the system prompt.

To list the associated keywords or arguments for a command, enter the **?** command in place of a keyword or argument on the command line. This form of help is called full help, because it lists the keywords or arguments that apply to the command based on the full command, keywords, and arguments you have already entered.

To obtain a list of commands or keywords that begin with a particular character string, enter the abbreviated command or keyword immediately followed by the **?** command. This form of help is called partial help, because it lists only the commands or keywords that begin with the abbreviation you entered.

Note: To enter the **?** character as part of a command, when it is not a request for online Help, enter the **Esc** character followed by the **?** character.

1.1.6 Examples

The following example displays exec commands available for a user with a privilege level of 6 (> prompt):

```
[local]Redback>?


 atm          ATM Operations
  debug        Modify debugging parameters
  disable      Drop into disable user mode
  edit         Edit a file with vi
  enable       Modify command mode privilege
  exit         Exit exec mode
  help         Description of the interactive help system
  monitor      Monitor information
  more         Display the contents of a file
  mrinfo       Request multicast router information
  mtrace       Trace reverse multicast path from source to receiver
  no           Disable an interactive option
  ping         Packet Internet Groper Command
  show         Show running system information
  ssh          Execute SSH/SSHD commands
  talk         talk to user
  telnet       Telnet to a host
  terminal     Modify terminal settings
  traceroute   Trace route to destination
```

The following example displays how to use partial help to display all commands (in global configuration mode) that begin with the character sequence `sy:`

```
[local]Redback(config)#sy?

  system    system clock-source
```

The following example displays how to use full help to display the next argument of a partially complete **system clock** command (in global configuration mode):

```
[local]Redback(config)#system clock ?

  summer-time   Configure summer (daylight savings) time
  timezone      Configure time zone
[local]Redback(config-ctx)#system clock
```

The following example displays the first few commands available for an administrator with a default privilege level of 6 (> prompt):

```
[local]Redback>?

bulkstats       Manage bulk statistics collection file
disable         Drop into disable administrator mode
enable          Modify command mode privilege
...
```

The following example shows how to use partial help to display all commands (in global configuration mode) that begin with the character sequence `sy`:

```
[local]Redback(config)#sy?

  system    system clock-source
```

The following example shows how to use full help to display the next argument of a partially complete **system clock** command (in global configuration mode):

```
[local]Redback(config)#system clock ?

  summer-time   Configure summer (daylight savings) time
  timezone      Configure time zone


[local]Redback(config-ctx)#system clock
```

1.2 aaa accounting administrator

aaa accounting administrator {**radius** |**tacacs+**}

{**no** | **default**} **aaa accounting administrator** {**radius** | **tacacs+**}

1.2.1 Purpose

Enables accounting messages for administrator sessions.

1.2.2 Command Mode

Context configuration

1.2.3 Syntax Description

radius	Specifies that accounting messages are to be sent to a Remote Authentication Dial-In User Service (RADIUS) server.
tacacs+	Specifies that accounting messages are to be sent to a Terminal Access Controller Access Control System Plus (TACACS+) server.

1.2.4 Default

Accounting is disabled.

1.2.5 Usage Guidelines

Use the **aaa accounting administrator** command to enable accounting messages for administrator sessions. Messages can be sent to a RADIUS or TACACS+ server.

You must configure at least one accounting server in the current context before any messages can be sent to it:

- To configure a TACACS+ server, use the **tacacs+ server** command (in context configuration mode); for more information, see *Configuring TACACS+*.
- To configure a RADIUS server, use the **radius server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to disable RADIUS or TACACS+ accounting messages for administrator sessions.

1.2.6 Examples

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

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

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
```

1.3 aaa accounting commands

aaa accounting commands *level* **tacacs+** [**except** *except-level*]

{**no** | **default**} **aaa accounting commands** *level*

1.3.1 Purpose

Specifies that accounting messages are sent to a Terminal Access Controller Access Control System Plus (TACACS+) server whenever an administrator enters commands at the specified privilege level (or higher).

1.3.2 Command Mode

Context configuration

1.3.3 Syntax Description

level	Command privilege level. The range of values is 0 to 15.
tacacs+	Indicates that a TACACS+ server must record commands for accounting.
except *except-level*	Optional. Command privilege level that will not be sent to the server for accounting. The range of values is 1 to 15. The value for this argument must be greater than that specified for the *level* argument.

1.3.4 Default

No TACACS+ accounting of commands is required.

1.3.5 Usage Guidelines

Use the **aaa accounting commands** command to specify that accounting messages are sent to a TACACS+ server whenever an administrator enters commands at the specified privilege level (or higher).

To use TACACS+, you must configure the IP address or hostname of a TACACS+ server in the context in which commands are accessed. To configure the server's IP address or hostname, use the **tacacs+ server** command (in context configuration mode); see *Configuring TACACS+*.

For information about default privilege levels for commands and how to modify command privilege levels, see *Performing Basic Configuration Tasks*.

Use the **no** or **default** form of this command to disable the sending of accounting messages to the TACACS+ server.

1.3.6 Examples

The following example shows how to send accounting messages to a TACACS+ server for commands that are configured with a privilege level of 6 or greater with the exception of privilege level 15:

```
[local]Redback(config-ctx)#aaa accounting commands 6 tacacs+ except 15
```

1.4 aaa accounting event

aaa accounting event {**dhcp** | **dhcpv6** | **dual-stack** | **reauthorization** | **ancp**}

{**no** | **default**} **aaa accounting event** {**dhcp** | **dhcpv6** | **dual-stack** | **reauthorization** | **ancp**}

1.4.1 Purpose

Enables accounting messages for Dynamic Host Configuration Protocol (DHCP) leases, DHCPv6 prefix delegation, IPv4 or IPv6 single-stack to dual-stack or dual-stack to single-stack transitions, reauthorization information, or Access Node Control Protocol (ANCP) events for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

1.4.2 Command Mode

Context configuration

1.4.3 Syntax Description

dhcp	
dhcpv6	Enables accounting messages to be sent whenever a DHCP lease is created or released.
dual-stack	Enables inclusion of prefix delegation transition events in event accounting messages sent for single-stack and dual-stack subscriber sessions when dynamic assignment or release of IPv6 host addresses occurs through DHCPv6.
reauthorization	Enables accounting messages to be sent for subscriber reauthorization sessions. Information sent provides details about subscriber circuits after reauthorization is complete.
ancp	Enables accounting messages to be sent whenever an ANCP event is received. Information sent provides details from the digital subscriber line access multiplexer (DSLAM) about changes to the subscriber DSL, such as a rate change.

1.4.4 Default

RADIUS-based accounting is disabled.

1.4.5 Usage Guidelines

Use the **aaa accounting event** command to enable accounting messages for DHCP leases, DHCPv6 prefix delegation assignment and release, IPv4 and IPv6 single-stack to dual-stack and dual-stack to single-stack transitions, reauthorization information, or ANCP events for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

Note: You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

If an ANCP event occurs when no subscriber session is on the line, no accounting message is sent.

Use the **no** or **default** form of this command to disable sending of RADIUS-based accounting messages.

1.4.6 Examples

The following example enables accounting messages for reauthorization information for subscriber sessions in the corpA context to be sent to the RADIUS accounting server with an IP address or hostname in the same context:

```
[local]Redback(config)#context corpA
[local]Redback(config-ctx)#aaa accounting event reauthorization
```

The following example enables accounting messages for DHCPv6 prefix delegation assignment and release information for subscriber sessions in the corpA context to be sent to the RADIUS accounting server with an IP address or hostname in the same context:

```
[local]Redback(config)#context corpA
[local]Redback(config-ctx)#aaa accounting event dhcpv6
[local]Redback(config-ctx)#aaa accounting subscriber radius
[local]Redback(config-ctx)#radius server 10.13.48.230 key TopSecret
```

1.5 aaa accounting l2tp

aaa accounting l2tp session {**none** | **radius** | **global**}

{**no** | **default**} **aaa accounting l2tp session** {**radius** | **global**}

Enables accounting messages for L2TP tunnels:

aaa accounting l2tp tunnel {**none** | **radius**}

{**no** | **default**} **aaa accounting l2tp tunnel**

1.5.1 Purpose

Enables accounting messages for Layer 2 Tunneling Protocol (L2TP) tunnels, or sessions in L2TP tunnels, or both, for the current context, to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. Enables accounting messages for sessions in L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context, local context, or both contexts.

1.5.2 Command Mode

Context configuration

1.5.3 Syntax Description

none	Disables RADIUS-based accounting.
radius	Enables RADIUS-based accounting.
global	Enables global RADIUS-based accounting (without global RADIUS authentication) for sessions in L2TP tunnels.

1.5.4 Default

RADIUS-based accounting is disabled.

1.5.5 Usage Guidelines

Use the **aaa accounting l2tp** to enable accounting messages for L2TP tunnels, or sessions in L2TP tunnels, or both, for the current context, to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. You can also enable accounting messages for sessions in L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context, local context, or both contexts.

Use the **aaa accounting l2tp tunnel** command with the **radius** keyword to enable accounting messages for L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. Use the **aaa accounting l2tp** command with the **session** and **radius** keywords to enable accounting messages for sessions in L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context. Both implementations of the **aaa accounting l2tp** command here reflect context-level L2TP accounting.

Use the **aaa accounting l2tp** command with the **session** and **global** keywords to enable accounting messages for sessions in L2TP tunnels for the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. This implementation reflects global-level L2TP accounting.

Note: If enabling context-level L2TP accounting, you must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. If enabling global-level L2TP accounting, you must configure at least one RADIUS accounting server in the local context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Two-stage accounting permits data for all contexts to be sent to both the RADIUS accounting servers in the local context for global-level accounting and any RADIUS accounting servers in the context to which the subscriber is bound

for context-level accounting. Enabling two-stage accounting for L2TP tunnels requires that you configure one or more RADIUS accounting servers in the local context and configure one or more RADIUS accounting servers in a nonlocal context or current context. You must also configure global L2TP accounting and global authentication. With two-stage accounting for sessions in L2TP tunnels, global authentication is optional. To enable two-stage accounting with global authentication, configure the **aaa accounting l2tp** command (in context configuration mode) with the **radius** keyword and the **aaa global accounting l2tp-session** command (in global configuration mode). To enable two-stage accounting without global authentication, use the **aaa accounting l2tp** command with the **session**, **radius**, and **global** keywords. The **global** keyword allows accounting to be performed without global authentication.

Note: When using global-level L2TP accounting, you must enable global L2TP accounting; use the **aaa global accounting l2tp-session** command.

Note:

If the SmartEdge router is acting as an L2TP network server (LNS) in a context, the accounting data is for the LNS; if it is acting as an L2TP access concentrator (LAC), the accounting data is for the LAC. If the SmartEdge router is acting as a tunnel switch, both sets of accounting data are sent to the RADIUS server; in this case, each set of data is tagged as follows:

- LNS accounting data (facing the LAC)—tag 1
- LAC accounting data (facing the LNS)—tag 2

Use the **no** or **default** form of this command or the **none** keyword to disable the sending of RADIUS accounting messages.

1.5.6 Examples

The following example shows how to enable accounting messages for L2TP tunnels in the `siteA` context to be sent to the RADIUS accounting server configured in the `siteA` context:

```
[local]Redback(config)#context siteA
[local]Redback(config-ctx)#aaa accounting l2tp radius
```

The following example shows how to enable accounting messages for sessions in L2TP tunnels in the `siteB` context to be sent to the RADIUS accounting server configured in the `local` context:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius accounting server 1.1.1.1 key my_key
.
.
.
[local]Redback(config)#context siteB
[local]Redback(config-ctx)#aaa accounting l2tp global
```

1.6 aaa accounting reauthorization subscriber

aaa accounting reauthorization subscriber {**none** | **radius**}

{**no** | **default**} **aaa accounting reauthorization subscriber**

1.6.1 Purpose

Enables accounting messages for the **reauthorize** command entered in the current context in exec mode to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the same context.

1.6.2 Command Mode

Context configuration

1.6.3 Syntax Description

none	Disables RADIUS-based accounting.
radius	Enables RADIUS-based accounting messages to be sent.

1.6.4 Default

RADIUS-based accounting is disabled.

1.6.5 Usage Guidelines

Use the **aaa accounting reauthorization** command to enable accounting messages for the **reauthorize** command entered in the current context in exec mode to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

Note: You must configure at least one RADIUS accounting server in the current context before any messages can be sent to it. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command or the **none** keyword to disable the sending of RADIUS accounting messages.

1.6.6 Examples

The following example shows how to enable accounting messages for subscriber reauthorization in the corpA context to be sent to the RADIUS server configured in the corpA context:

```
[local]Redback(config)#context corpA
[local]Redback(config-ctx)#aaa accounting reauthorization radius
```

1.7 aaa accounting subscriber

aaa accounting subscriber {**none** | **radius [attribute-guided]** | **global**}

{**no** | **default**} **aaa accounting subscriber** {**radius** | **global**}

1.7.1 Purpose

Enables accounting messages for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context (for context-level subscriber accounting), in the local context (for global-level subscriber accounting), or in both contexts (for context- and global-level subscriber accounting).

1.7.2 Command Mode

Context configuration

1.7.3 Syntax Description

none	Disables RADIUS-based accounting.
radius	Enables RADIUS-based accounting.

attribute-guided	Enables attribute-guided RADIUS-based accounting; ensures that the RADIUS accounting server can send and receive accounting packets. Accounting packets are sent to a subscriber only when the Accounting-Mode VSA is present in the authentication response received from the subscriber.
global	Enables global RADIUS-based accounting (without global RADIUS authentication).

1.7.4 Default

RADIUS-based accounting is disabled.

1.7.5 Usage Guidelines

Use the **aaa accounting subscriber** command to enable accounting messages for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context (for context-level subscriber accounting), in the local context (for global-level subscriber accounting), or in both contexts (for context- and global-level subscriber accounting).

Use the **aaa accounting subscriber** command with the **radius** keyword to enable accounting messages for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the same context.

Use the **aaa accounting subscriber** command with the **global** keyword to enable accounting messages for subscriber sessions in the current context to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Note: If enabling context-level subscriber accounting, you must configure at least one RADIUS accounting server in the current context before any messages can be sent to the server. If enabling global-level subscriber accounting, you must configure at least one RADIUS accounting server in the local context before any messages can be sent to the server. To configure the server, use the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

To enable two-stage accounting, configure one or more RADIUS accounting servers in a nonlocal context and configure one or more RADIUS accounting servers in the local context. With two-stage accounting, global authentication is optional. To enable two-stage accounting with global authentication, configure global authentication by using the **radius** keyword with the **aaa authentication subscriber** command (in context configuration mode) and the **aaa global authentication subscriber** command (in

global configuration mode). To enable two-stage accounting without global authentication, configure the keywords **radius** and **global** with the **aaa accounting subscriber** command. In two-stage accounting, data for all contexts is sent to both the RADIUS accounting servers in the local context and to any RADIUS accounting servers in the context to which the subscriber is bound.

When configuring global accounting for subscriber sessions, be aware that the **aaa accounting subscriber global** and aaa global accounting event commands are interdependent. To enable global accounting for subscriber sessions, you must:

1 Configure the **aaa accounting subscriber global** command in the desired context or contexts. (Accounting messages for subscriber sessions in this context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.)

2 Configure the **aaa global accounting event** command in global configuration mode, outside of any context. This command applies to all contexts that have the **aaa accounting subscriber global** command configured.

Global accounting is not enabled for contexts that do not have the **aaa accounting subscriber global** command configured, regardless of whether the **aaa global accounting event** command is configured in global configuration mode.

Note: To use global-level subscriber accounting, you must enable it; use the **aaa global accounting subscriber** command.

Note: The **aaa accounting subscriber** command can only enable the sending of accounting packets that include packet and byte counts for a circuit if the **counters** command is configured in the Asynchronous Transfer Mode (ATM) profile referenced by the circuit to which the subscriber is bound; for more information about ATM profiles, see *Configuring Circuits*.

Note: The SmartEdge router does not send the RADIUS accounting packet for a Point-to-Point Protocol (PPP) subscriber until the session completes the IP Control Protocol (IPCP) stage of PPP. Delaying the start record ensures that standard RADIUS attribute 8, Framed-IP-Address, is populated.

Use the **no** or **default** form of this command or the **none** keyword to disable the sending of RADIUS accounting messages.

1.7.6 Examples

The following example shows how to enable accounting messages for subscriber sessions in the `siteA` context to be sent to the RADIUS accounting server configured in the `siteA` context:

```
[local]Redback(config)#context siteA
[local]Redback(config-ctx)#aaa accounting subscriber radius
```

The following example shows how to enable accounting messages for subscriber sessions in the `siteB` context to be sent to the RADIUS accounting server configured in the `local` context and to the RADIUS accounting server configured in the `siteB` context:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius accounting server 1.1.1.1 key my_key
.
.
.
[local]Redback(config)#context siteB
[local]Redback(config-ctx)#aaa accounting subscriber radius global
```

The following example shows how to configure RADIUS-based attribute-guided accounting. This configuration is used if the accounting_mode is set for the subscriber:

```
[local]Redback(config-ctx)#radius accounting server 1.1.1.1 key redback
[local]Redback(config-ctx)#aaa accounting subscriber radius attribute-guided
```

1.8 aaa accounting suppress-acct-on-fail

aaa accounting suppress-acct-on-fail [**except-for** {[**duplicate-ip**][**no-l2tp-peer**][**slid-session-limit**]]}

{**no** | **default**} **aaa accounting suppress-acct-on-fail** [**except-for** {[**duplicate-ip**][**no-l2tp-peer**][**slid-session-limit**]]}

1.8.1 Purpose

Suppresses the sending of accounting messages to RADIUS servers when a subscriber session cannot be established.

no | **default**

1.8.2 Command Mode

Context configuration

1.8.3 Syntax Description

duplicate-ip	Optional. Does not suppress accounting messages if the IP address specified in an Access Accept packet is already used by another subscriber.
no-l2tp-peer	Optional. Does not suppress accounting messages if the Layer 2 Tunneling Protocol (L2TP) peer cannot be reached and the session is not brought up.
slid-session-limit	Optional. Does not suppress accounting messages for the stop related to session-limit enforcement during post-authentication.

1.8.4 Default

RADIUS-based accounting is disabled. When RADIUS-based accounting is enabled using the **aaa accounting subscriber** command (in context configuration mode), the operating system always sends an accounting record when a subscriber session cannot be established.

1.8.5 Usage Guidelines

Use the **aaa accounting suppress-acct-on-fail** command to suppress sending accounting messages to RADIUS accounting servers when a subscriber session cannot be established due to an authentication problem, a changed IP address, and so on.

You can specify any condition for which accounting messages is not suppressed, but the conditions must be entered in the order shown above.

Use the **no** or **default** form of this command to suppress sending accounting messages when any error condition occurs.

1.8.6 Examples

The following example shows how to suppress accounting messages sent to RADIUS accounting servers except when the L2TP peer for a subscriber session cannot be reached and the session not established:

```
[local]Redback(config-ctx)#aaa accounting suppress-acct-on-fail
except-for no-l2tp-peer
```

The following example shows how to suppress accounting messages sent to RADIUS accounting servers except when the L2TP peer for a subscriber session cannot be reached and the session not established or in the case of session-limit enforcement. :

```
[local]Redback(config-ctx)#aaa accounting suppress-acct-on-fail
except-for no-l2tp-peer slid-session-limit
```

1.9 aaa authentication administrator

aaa authentication administrator {**[{console** | **vty}]** {***method***[***method***[***method***]]}} | **maximum sessions** ***num-sess***

{**no** | **default**} **aaa authentication administrator** {[{**console** | **vty**}] {***method***[***method***[***method***]]}} | **maximum**

1.9.1 Purpose

Prioritizes the methods available for authenticating administrators, or modifies the maximum number of administrator sessions that can be simultaneously active.

1.9.2 Command Mode

Context configuration

1.9.3 Syntax Description

console	Optional. Enables the specified administrator authentication method on the console port.
vty	Optional. Enables the specified administrator authentication method on a vty port, which is a virtual terminal port used for remote console access.

method	Authentication method, according to one of the following keywords: • **local**—Specifies authentication by the SmartEdge router configuration. • **radius**—Specifies authentication by a Remote Authentication Dial-In User Service (RADIUS) server. • **tacacs+**—Specifies authentication by a Terminal Access Controller Access Control System Plus (TACACS+) server. One method is required. Specifying a second or third method is optional. Separate each value with a space.
maximum sessions ***num-sess***	Maximum number of administrator sessions that can be active simultaneously. The range of values is 0 to 32. For the local context, the default value is 10. For nonlocal contexts, the default value is 1. The total number of active Telnet, Secure Shell (SSH), or both types of administrator sessions must be fewer than or equal to 100 for all configured contexts. In addition, one administrator session is supported for the console port.

1.9.4 Default

Authentication is performed by the SmartEdge router configuration and is permitted on both the console port and vty ports. For the local context, the number of administrator sessions that can be simultaneously active is 10; for nonlocal contexts, it is 0 or 1 (0 when no administrators are configured; 1 when administrators are configured).

1.9.5 Usage Guidelines

Use the **aaa authentication administrator** command to prioritize the available administrator authentication methods or modify the maximum number of administrator sessions that can be simultaneously active. If you use this command to prioritize the available administrator authentication methods, you can configure a port type for each specified authentication method.

Authentication methods are attempted in the order in which you enter the keywords. For example, if you enter the **radius** keyword first, followed by the **tacacs+** keyword, followed by the **local** keyword, authentication is first attempted by the RADIUS server, then by the TACACS+ server, and, finally, by the local configuration.

Note: If a RADIUS or TACACS+ server rejects the authentication of an administrator, authentication is not attempted by the next method. If, however, the RADIUS or TACACS+ server is unavailable or unreachable, authentication is attempted by the next method. Authentication by the SmartEdge router configuration is always available as a fallback, even when the **local** keyword is not specified. If the SmartEdge router configuration rejects an administrator, authentication is not attempted by the next method.

Note: Do not use both **console** and **vty** keywords within the same command line. It is not supported. This functionally is equivalent to the default behavior.

Note: To use RADIUS, the IP address or hostname of at least one RADIUS server must be configured in the context to which the administrator is to be bound. To configure the server's IP address or hostname, use the **radius server** command (in context configuration mode); for more information, see *Configuring RADIUS*. To use TACACS+, the IP address or hostname of a TACACS+ server must be configured in the context to which the administrator is to be bound. To configure the server's IP address or hostname, use the **tacacs+ server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Note: The total number of simultaneous, active Telnet and SSH administrator sessions must be less than or equal to 20 on the system as a whole (that is, for all configured contexts).

The maximum number of administrator SSH sessions that can be simultaneously active for all configured contexts can be configured through the **ssh server full-drop** command (in global configuration mode); the default value is 20. If there are active Telnet sessions, the maximum number of global SSH sessions is limited to the maximum number of SSH sessions configured through the **ssh server full-drop** command, minus the number of active Telnet sessions in all contexts.

Use the **no** or **default** form of this command to return to using only the SmartEdge router configuration for authentication of administrators.

1.9.6 Examples

The following example shows how to configure the console port of a SmartEdge router to authenticate administrators through a RADIUS server with the SmartEdge router configuration authentication (local database) as a backup:

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

The following example shows how to configure a vty port on a SmartEdge router to authenticate administrators through a TACACS+ server:

```
[local]Redback(config-ctx)#aaa authentication administrator vty tacacs+
```

The following example shows how to modify the number of administrator sessions that can be simultaneously active in the local context from `10` (the default) to `15`:

```
[local]Redback(config-ctx)#aaa authentication administrator maximum
sessions 15
```

1.10 aaa authentication subscriber

aaa authentication subscriber {**global** | **local** [{**global** | **none** | **radius** [{**global** | **local** | **none**}] | **none** | **radius**}}

{ **no** | **default**} **aaa authentication subscriber**

1.10.1 Purpose

Authenticates subscribers through the SmartEdge router configuration or through one or more Remote Authentication Dial-In User Service (RADIUS) server databases.

1.10.2 Command Mode

Context configuration

1.10.3 Syntax Description

global	When used alone, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context. When used as an optional keyword following **local**, first attempts subscriber authentication through the SmartEdge router configuration in the current context. In the event that no corresponding subscriber record is found in the local database, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context. When used as an optional keyword following **radius**, first attempts subscriber authentication through one or more RADIUS servers with IP addresses or hostnames configured in the current context. If those RADIUS servers are not reachable, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the local context.
local	When used alone, authenticates subscribers through the SmartEdge router configuration in the current context. When used as an optional keyword following **radius**, authenticates subscribers through one or more RADIUS servers with IP addresses or hostnames configured in the current context. If the RADIUS servers are not reachable, authenticates subscribers through the SmartEdge router configuration in the current context.
none	When used alone, specifies that authentication of subscribers is not required—all access succeeds. When used as an optional keyword following **local**, subscribers are first authenticated through the SmartEdge router configuration. In the event that no corresponding subscriber record is found in the local database, access succeeds.
radius	When used alone, authenticates subscribers by one or more RADIUS servers with IP addresses or hostnames in the current context. When used as an optional keyword following **local**, first attempts subscriber authentication through the SmartEdge router configuration in the current context. In the event that no corresponding subscriber record is found in the local database, authenticates subscribers by one or more RADIUS servers with IP addresses or hostnames in the current context.

1.10.4 Default

Subscribers are authenticated by the SmartEdge router configuration.

1.10.5 Usage Guidelines

Use the **aaa authentication subscriber** command to authenticate subscribers through the SmartEdge router configuration or through one or more RADIUS server databases.

The SmartEdge router configuration is also referred to as the “local database,” which is simply a set of commands, such as the **subscriber** command (in context configuration mode) and the **password** command (in subscriber configuration mode).

With RADIUS, the database records of the RADIUS server are used to authenticate subscribers. The IP address or hostname of one or more RADIUS servers can be configured in the “local” context or in the context to which the subscriber’s circuit is to be bound. Each context can use its own set of RADIUS servers for authentication. Alternatively, a context can be configured to use the RADIUS servers with IP addresses or hostnames configured in the “local” context—this is known as “global authentication.”

With global authentication, the RADIUS servers are expected to return the Context-Name vendor-specific attribute (VSA) that indicates the particular context to which the subscriber is to be bound. You can also configure the SmartEdge router to try authentication through one or more RADIUS servers with IP addresses or hostnames configured in the current context first, with a fallback to the global RADIUS server or to the local database, in case the RADIUS server configured in the current context becomes unreachable.

Note: To use RADIUS, the IP address or hostname of at least one RADIUS server must be configured in the local context or in the context to which the subscriber is to be bound. To configure the server’s IP address or hostname, use the **radius server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

To disable authentication of subscribers, use the **none** keyword with this command. Do this only when subscriber authentication is not required, such as when Dynamic Host Configuration Protocol (DHCP) is used to obtain IP addresses for subscribers’ hosts.

Caution!

Risk of security breach. With the **aaa authentication subscriber none** command, the SmartEdge router does not read any of the subscriber records configured, except for the default subscriber record. This means that individual subscriber usernames and passwords are not authenticated by the SmartEdge router. Therefore, IP addresses, routes, and Address Resolution Protocol (ARP) entries within individual subscriber records are not installed. Verify your network security setup before using the **aaa authentication subscriber none** command.

Use the **no** or **default** form of this command to authenticate subscribers through the SmartEdge router configuration.

1.10.6 Examples

The following example authenticates subscriber sessions for the `siteB` context by first using the RADIUS server configured within the context, followed by the SmartEdge router configuration for the context should the RADIUS server become unreachable:

```
[local]Redback(config)#context siteB
[local]Redback(config-ctx)#radius server 10.2.3.4 key TopSecret
[local]Redback(config-ctx)#aaa authentication subscriber radius local
```

1.11 aaa authorization commands

aaa authorization commands *level***tacacs+** [**none**] [**except** *except-level*]

{**no** | **default**} **aaa authorization commands** *level*

1.11.1 Purpose

Specifies that commands with a matching privilege level (or higher) require authorization through Terminal Access Controller Access Control System Plus (TACACS+).

1.11.2 Command Mode

Context configuration

1.11.3 Syntax Description

level	Privilege level. The range of values is 0 to 15. A user account with a privilege level that matches or is greater than the value of the ***level*** argument must be authorized by TACACS+ before the user can enter SmartEdge router CLI commands set to this privilege level.
tacacs+	Enforces authorization through TACACS+.
none	Optional. Disables authorization if the server is unavailable.
except ***except-level***	Optional. Command privilege level that will not be sent to the server for authorization. The range of values is 1 to 15. The value for this argument must be greater than that specified for the ***level*** argument.

1.11.4 Default

Commands do not require authorization through TACACS+.

1.11.5 Usage Guidelines

Use the **aaa authorization commands** command to specify that commands with a matching privilege level (or higher) require authorization through TACACS+.

Caution!

Risk of administrative failure. If a TACACS+ server has not been set up and configured before this command is issued, you may not have authorization to use commands on your SmartEdge router. To reduce the risk, you must first configure the IP address or hostname of a TACACS+ server in the context in which commands are accessed. To do so, enter the **tacacs+ server** command (in context configuration mode); for more information, see *Configuring TACACS+*.

Caution!

Risk of administrative failure. If you have configured authorization without the **none** keyword and the TACACS+ server is not available, you might not have authorization to use commands on your SmartEdge router. To reduce the risk, always include the **none** keyword when entering this command.

Caution!

Risk of administrative failure. If the administrator record on the TACACS+ server is set up to authorize only a limited set of commands, the administrator might not be allowed to perform critical tasks using the SmartEdge router. To reduce the risk, we recommend, therefore, that you configure at least one administrator record on the TACACS+ server that has authorization to access all commands.

Note: For information about default command privilege levels and how to modify them, see *Performing Basic System Tasks*.

Use the **no** or **default** form of this command to disable the requirement for TACACS+ authorization.

1.11.6 Examples

The following example shows how to specify that TACACS+ authorization is required in the `restricted` context for the use of commands with privilege levels of `10` or higher with the exception of privilege level `15`:

```
[restricted]Redback(config)#configure
[restricted]Redback(config-ctx)#aaa authorization commands 10 except 15
```

The following example shows how to specify that TACACS+ authorization is required in the `restricted` context for all commands:

```
[restricted]Redback(config)#configure
[restricted]Redback(config-ctx)#aaa authorization commands 0 tacacs+
```

1.12 aaa authorization tunnel

aaa authorization tunnel {**none** | **radius**}

{**no** | **default**}**aaa authorization tunnel** {**none** | **radius**}

1.12.1 Purpose

Specifies the type of authorization for Layer 2 Tunneling Protocol (L2TP) peers.

1.12.2 Command Mode

Context configuration

1.12.3 Syntax Description

none	Specifies that L2TP peers are authorized by the local configuration.
radius	Specifies that L2TP peers are authorized by a Remote Authentication Dial-In User Service (RADIUS) server.

1.12.4 Default

L2TP peers are authorized by the SmartEdge router configuration.

1.12.5 Usage Guidelines

Use the **aaa authorization tunnel** command to specify the type of authorization for L2TP peers.

Use the **no** or **default** form of this command to specify the default behavior.

1.12.6 Examples

The following example shows how to configure the `local` context to authorize L2TP peers by a RADIUS server:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa authorization tunnel radius
```

1.13 aaa double-authentication subscriber radius

aaa double-authentication subscriber radius [**none** [**profile** ***profile-name***]]

no aaa double-authentication subscriber radius [**none** [**profile** ***profile-name***]]

1.13.1 Purpose

Reauthenticates subscribers through the specified Remote Authentication Dial-In User Service (RADIUS) server database.

1.13.2 Command Mode

Context configuration

1.13.3 Syntax Description

none	Optional. Specifies that no second authentication is to take place if the RADIUS server is unavailable.
profile ***profile-name***	Optional. Defines a local profile used when the second RADIUS server is unavailable; also referred to as the fallback profile.

1.13.4 Default

Subscribers are authenticated one time, either through the SmartEdge router configuration or through one of the RADIUS server databases.

1.13.5 Usage Guidelines

Use the **aaa double-authentication subscriber radius** command to specify reauthentication through the specified RADIUS server database, and optionally, to define a local profile to be used when the second RADIUS server is unavailable.

RADIUS provisioning is enhanced so that subscribers can be authenticated twice without a RADIUS proxy server. Subscribers are first authenticated by a global RADIUS server and then by the RADIUS server for the binding context.

When the SmartEdge router receives the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) Auth-Req packet, it sends a RADIUS Access-Request packet to the global RADIUS server configured for the local context. If the Access-Accept packet returned by the RADIUS server indicates that the subscriber is to be reauthenticated, the SmartEdge router sends a second Access-Request packet to the RADIUS server for the binding (nonlocal) context specified by the global server. Depending on the response of the second server, the session is either terminated or tunneled using a list of attributes consolidated from both RADIUS responses. Attribute values received from the second RADIUS server override values received from the first server and values configured locally in the nonlocal context.

If the configured authentication failover method is none and the second RADIUS server is unavailable, the subscriber is provisioned using the local profile (specified with the `profile` keyword) plus the attributes received from the first RADIUS server, and the subscriber is not reauthenticated.

Note:

Attribute processing is performed in the following order:

- Service provider RADIUS
- Global RADIUS
- Service provider defined profile (local or fallback profile)
- Service provider default subscriber profile

Use the **no** form of this command to disable the requirement for reauthenticating subscribers through the specified RADIUS server database.

1.13.6 Examples

The following example shows how to configure the context `ISP3` to reauthenticate its subscriber sessions using the RADIUS server with the IP address `155.53.44.181` configured in the `local` context:

```
[local]Redback(config-ctx)#aaa global authentication subscriber radius
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius accounting server 155.53.44.181
encrypted-key 3828082561D6BDD6
[local]Redback(config)#context ISP3
[local]Redback(config-ctx)#aaa authentication subscriber global
[local]Redback(config-ctx)#aaa double-authentication subscriber
radius none profile last
[local]Redback(config-ctx)#radius server 155.53.44.181 encrypted-key
3828082561D6BDD6 oldports subscriber profile last
[local]Redback(config-sub)#ip address pool
```

1.14 aaa encrypted-password default

aaa encrypted-password default ***password***

no aaa encrypted-password default

1.14.1 Purpose

Changes the default AAA authentication and authorization password to the specified encrypted password.

1.14.2 Command Mode

Context configuration

1.14.3 Syntax Description

password	Alphanumeric string representing a default authentication and authorization password. This password is encrypted. Control characters are not allowed.

1.14.4 Default

The default AAA authentication and authorization password is “Redback”.

1.14.5 Usage Guidelines

Use the **aaa encrypted-password default** command to change the default authentication and authorization password to the specified encrypted password. This new default AAA password is saved in the encrypted form as well. When you enter the show configuration command, the display shows the default AAA password in the encrypted form.

Use the **no** form of this command to restore the default password of “Redback”.

1.14.6 Examples

The following example shows how to configure the new default AAA encrypted password of F9BFC75FC9F3F8AD:

```
[local]Redback(config-ctx)#aaa encrypted-password
default F9BFC75FC9F3F8AD
```

1.15 aaa global accounting event

aaa global accounting event {**dhcp** | **dhcpv6** | **dual-stack** | **reauthorization** | **ancp**}

{**no** | **default**} **aaa global accounting event** {**dhcp** | **dhcpv6** | **dual-stack** | **reauthorization** | **ancp**}

1.15.1 Purpose

Enables accounting messages for DHCP leases, IPv4 or IPv6 single-stack to dual-stack or dual-stack to single-stack transitions, DHCPv6 prefix delegation,

reauthorization information, or ANCP events for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

1.15.2 Command Mode

Global configuration

1.15.3 Syntax Description

dhcp	Enables accounting messages to be sent whenever a DHCP lease is created or released.
dhcpv6	Enables inclusion of prefix delegation transition events in event accounting messages sent for single-stack and dual stack subscriber sessions when dynamic assignment or release of IPv6 host addresses occurs through DHCPv6.
dual-stack	Enables accounting messages to be sent during a subscriber session when the IPv4 or IPv6 stack transitions up or down. This allows a single-stack subscriber session to become dual-stack or a dual-stack session to become single-stack.
reauthorization	Enables accounting messages to be sent for subscriber reauthorization sessions. The information sent provides details about subscriber circuits after reauthorization is completed.
ancp	Enables accounting messages to be sent whenever an ANCP event is received. The information sent provides details from the DSLAM about changes, such as a rate change, to the subscriber DSL.

1.15.4 Default

RADIUS-based accounting is disabled.

1.15.5 Usage Guidelines

Use the **aaa global accounting event** command to enable accounting messages for DHCP leases, IPv4 or IPv6 single-stack to dual-stack or dual-stack to single-stack transitions, reauthorization information, IPv4 or IPv6 stack transitions, or ANCP events for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

If an ANCP event occurs when no subscriber session is on the line, accounting messages are not sent.

When configuring global accounting for subscriber sessions, be aware that the **aaa accounting subscriber global** and **aaa global accounting event** commands are interdependent. To enable global accounting for subscriber sessions, you must first configure the **aaa accounting subscriber global** command:

1. Configure the **aaa accounting subscriber global** command in the desired contexts. (Accounting messages for subscriber sessions in the context are sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.)
2. Configure the **aaa global accounting event** command in global configuration mode, outside of any context. This command applies to all contexts that have the **aaa accounting subscriber global** command configured.

Use the **no** or **default** form of this command to disable RADIUS-based accounting.

1.15.6 Examples

The following example enables accounting messages for reauthorization information for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context:

```
[local]Redback(config)#aaa global accounting event reauthorization
```

The following example enables accounting messages for DHCPv6 prefix delegation assignment or release information for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context:

```
[local]Redback(config)#aaa global accounting event dhcpv6
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa accounting subscriber global
[local]Redback(config-ctx)#radius server 10.13.48.230 key TopSecret
```

1.16 aaa global accounting l2tp-session

aaa global accounting l2tp-session radius context local

{**no** | **default**} **aaa global accounting l2tp-session**

1.16.1 Purpose

Enables accounting messages for Layer 2 Tunneling Protocol (L2TP) tunnels or sessions in L2TP tunnels in all contexts to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

1.16.2 Command Mode

Global configuration

1.16.3 Syntax Description

`radius context local`	Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the local context.

1.16.4 Default

The SmartEdge router does not send accounting messages to a RADIUS server.

1.16.5 Usage Guidelines

Use the **`aaa global accounting l2tp-session`** command to enable accounting messages for L2TP tunnels or sessions in L2TP tunnels in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Note: To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **`radius accounting server`** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **`no`** or **`default`** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge router configuration.

1.16.6 Examples

The following example shows how to configure the system to send accounting messages for L2TP sessions in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the `local` context:

```
[local]Redback(config)#aaa global accounting l2tp-sessio
n radius context local
```

1.17 aaa global accounting reauthorization subscriber

aaa global accounting reauthorization subscriber radius context local

{**no** | **default**} **aaa global accounting reauthorization subscriber**

1.17.1 Purpose

Enables accounting messages for the **reauthorize** command entered in any context in exec mode to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

1.17.2 Command Mode

Global configuration

1.17.3 Syntax Description

radius context local	Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the `local` context.

1.17.4 Default

RADIUS-based accounting is disabled.

1.17.5 Usage Guidelines

Use the **aaa global accounting reauthorization subscriber** command to enable accounting messages for the **reauthorize** command entered in any context in exec mode to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context. These messages indicate that subscriber reauthorization has been completed.

Note: To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge router configuration.

1.17.6 Examples

The following example shows how to configure the system to send accounting messages for subscriber reauthorization in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the `local` context:

```
[local]Redback(config)#aaa global accounting reauthorization subscriber
radius context local
```

1.18 aaa global accounting subscriber

aaa global accounting subscriber radius context local

{**no** | **default**} **aaa global accounting subscriber**

1.18.1 Purpose

Enables accounting messages for subscriber sessions in all contexts to be sent to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

1.18.2 Command Mode

Global configuration

1.18.3 Syntax Description

radius context local	Indicates accounting messages are sent by RADIUS accounting servers with IP addresses or hostnames configured in the local context.

1.18.4 Default

The SmartEdge router does not send subscriber session accounting messages to a RADIUS server.

1.18.5 Usage Guidelines

Use the **aaa global accounting subscriber** command to enable accounting messages for subscriber sessions in all contexts to be sent to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Note: To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to return the system to its default behavior of performing accounting based on the SmartEdge router configuration.

1.18.6 Examples

The following example shows how to configure the system to send accounting messages for subscriber sessions in all contexts to one or more RADIUS servers with IP addresses or hostnames configured in the `local` context:

```
[local]Redback(config)#aaa global accounting subscriber radius context
local
```

1.19 aaa global authentication subscriber

aaa global authentication subscriber radius context local

{**no** | **default**} **aaa global authentication subscriber**

1.19.1 Purpose

Enables global subscriber authentication through one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the local context.

1.19.2 Command Mode

Global configuration

1.19.3 Syntax Description

radius context local	Indicates authentication is performed by the RADIUS servers with IP addresses or hostnames configured in the local context.

1.19.4 Default

The SmartEdge router does not send subscriber authentication messages to a RADIUS server.

1.19.5 Usage Guidelines

Use the **aaa global authentication subscriber** command to enable global subscriber authentication through one or more RADIUS servers with IP addresses or hostnames configured in the local context.

Note: To use RADIUS, you must configure the IP address or hostname of at least one RADIUS server in the local context. To configure the server's IP address or hostname, enter the **radius server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to disable global subscriber authentication.

1.19.6 Examples

The following example shows how to configure the context `siteA` to globally authenticate its subscriber sessions using the RADIUS server with the IP address of `10.2.3.4` configured in the `local` context:

```
[local]Redback(config)#aaa global authentication subscri
ber radius context local
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius server 10.2.3.4 key TopSecret
[local]Redback(config)#context siteA
[local]Redback(config-ctx)#aaa authentication subscriber global
```

1.20 aaa global coa ignore rse-attr-stack-mismatch

aaa global coa ignore rse-attr-stack-mismatch

{**no** | **default**} **aaa global coa ignore rse-attr-stack-mismatch**

1.20.1 Purpose

Configures global change-of-authorization (CoA) options. During CoA, this command permits service activation in case of stack mismatch. It ignores service that is not relevant and any stack information or part that is not present in the session. It also sends the regular service start, interim, and stop accounting, even if the service cannot be activated.

1.20.2 Command Mode

Global configuration

1.20.3 Syntax Description

This command has no keywords or arguments.

1.20.4 Default

By default, this command is not enabled, and RSE service activation via COA is acked or rejected based on the stack information within the access accept. In a dual-stack case, if an IPv4 stack subscriber is up but IPv6 is down and an RSE is applied that contains both IPv4 and IPv6 attributes via CoA, all IPv4 attributes are applied and all IPv6 attributes are saved, marked as not applied. In a single-stack case, if an IPv4 stack subscriber is up and an RSE that contains both IPv4 and IPv6 attributes is applied via CoA, it is rejected and a NAK is sent to RADIUS, and the IPv6 attributes are not saved. The single-stack IPv4-capable subscriber does not have the option to bring up the IPv6 stack. When AAA processes the attributes in the service, it checks every attribute stack type against the session stack. If a single attribute fails, it fails the entire CoA process.

1.20.5 Usage Guidelines

Use the **`aaa global coa ignore rse-attr-stack-mismatch`** command to ignore service that is not relevant and if the stack information or part is not present in the session. When this command is enabled, the regular service start, interim, and stop accounting is sent, even if the service cannot be activated.

The results of enabling this command include the following::

- Service activation or deactivation through CoA is always acknowledged when a stack mismatch occurs.
- IPv6 or dual-stack RSE can be activated on a single-stack IPv4 or IPv6 session.
- A combination of services can be attached to a given session.

1.21 aaa global reject empty-username

aaa global reject empty-username

{**no** | **default**} **aaa global reject empty-username**

1.21.1 Purpose

Suppresses RADIUS access-request messages when no username is specified.

1.21.2 Command Mode

Global configuration

1.21.3 Syntax Description

This command has no keywords or arguments.

1.21.4 Default

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

1.21.5 Usage Guidelines

Use the **aaa global reject empty-username** command to suppress RADIUS Access-Request messages when no username is specified. The relevant attribute in the Access-Request message is the User-Name attribute. The operating system logs an informational message that identifies the circuit, then discards the Access-Request packet.

Use the **no** or **default** form of this command to restore the default behavior of sending Access-Request messages to the RADIUS server regardless of whether a username is specified.

1.21.6 Examples

The following example shows how to configure the SmartEdge router to suppress Access-Request messages when no username is specified:

```
[local]Redback(config)#aaa global reject empty-username
```

1.22 aaa global route-download

aaa global route-download radius context local

no aaa global route-download

1.22.1 Purpose

Configures a global route download server.

1.22.2 Command Mode

Global configuration

1.22.3 Syntax Description

This command has no keywords or arguments.

1.22.4 Default

The SmartEdge router does not send route download messages to a RADIUS server.

1.22.5 Usage Guidelines

This command is used to enable the global route download method.

1.22.6 Examples

The following example shows how to initiate route download in the aaa global mode:

```
[local]Redback(config)#aaa global route-download context local
```

1.23 aaa global session-id-count

aaa global session-id-count

{no | default} aaa global session-id-count

1.23.1 Purpose

Changes the account session ID rules to comply with the requirements of a short acct-session-id. The shortened acct-session-id is eight characters long and should be used for accounting purposes only.

1.23.2 Command Mode

Global configuration

1.23.3 Syntax Description

This command has no keywords or arguments.

1.23.4 Default

By default, vendor-specific account session ID rules are disabled.

1.23.5 Usage Guidelines

Use the **`aaa global session-id-count`** command to change the account session ID rules to comply with the requirements of vendor-specific equipment. When you apply this command, the SmartEdge router enforces the following rules:

- The account session ID attribute is a unique hexadecimal number.
- The first session is number zero (0) and subsequent sessions increment by one (1) until the value FFFFFFFF is reached. Upon process restart or failover, the count of the session begins with the value after the previous value is reached.
- After the value FFFFFFFF is reached, renumbering from zero begins.
- When the SmartEdge router receives an accounting request, it sends an account session ID.

The operating system supports this feature in the following environments:

- L2TP (LAC/LNS)
- PPPoE
- PPPoA
- PPPoEoA
- PPPoEoE

To use this feature, configure the RADIUS and RADIUS accounting on an SmartEdge router, and then configure a RADIUS accounting server.

Use the **no** or the **default** form of this command to reset the **aaa global session-id-count** command to the default account session ID rules.

1.23.6 Examples

The following example shows how to globally configure the SmartEdge router so that the account session ID rules comply with the requirements of vendor-specific equipment:

```
[local]Redback(config)#aaa global session-id-count
```

1.24 aaa global suppress-authentication slid-session-limit

aaa global suppress-authentication slid-session-limit

{**no** | **default**} **aaa global suppress-authentication slid-session-limit**

1.24.1 Purpose

Prevents a session from being established when the maximum configured number of sessions has been established. .

1.24.2 Command Mode

Global configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

By default, session-limit enforcement is only performed after authentication is successful.

1.24.5 Usage Guidelines

Use the **aaa global supress-authentication slid-session-limit** command to prevent the SmartEdge router from trying to authenticate a session after the maximum number of sessions has already been established.

1.24.6 Examples

The following example globally configures the SmartEdge router so that no authentication request is sent to the RADIUS server when the maximum number of sessions has been established.

```
[local]Redback(config)#aaa global suppress-authenticat
ion slid-session-limit
```

1.25 aaa global update subscriber

aaa global update subscriber ***interval***

{**no** | **default**} **aaa global update subscriber**

1.25.1 Purpose

Sends updated accounting records for subscribers in all contexts to one or more Remote Authentication Dial-In User Service (RADIUS) accounting servers with IP addresses or hostnames configured in the local context.

1.25.2 Command Mode

Global configuration

1.25.3 Syntax Description

interval	Period (in minutes) between accounting updates. The range of values is 10 to 10,080.

1.25.4 Default

This authentication, authorization, and accounting (AAA) feature is disabled.

1.25.5 Usage Guidelines

Use the **aaa global update subscriber** command to send updated accounting records for subscribers in all contexts to one or more RADIUS accounting servers with IP addresses or hostnames configured in the local context.

Note: You must configure accounting using the **aaa global accounting subscriber** command (in global configuration mode).

Note: To use RADIUS, you must configure the IP address or hostname of at least one RADIUS accounting server in the local context. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to disable subscriber account updating.

1.25.6 Examples

The following example shows how to globally configure an update to be sent for all subscribers in the system when each subscriber's session comes up, and every 20 minutes thereafter, for as long as the subscriber session lasts:

```
[local]Redback(config)#aaa global update subscriber 20
```

1.26 aaa hint ip-address

aaa hint ip-address

no aaa hint ip-address

1.26.1 Purpose

Enables the SmartEdge router to notify the Remote Authentication Dial-In User Service (RADIUS) server that the IP address in the Framed-IP-Address attribute is the preferred IP address.

1.26.2 Command Mode

Context configuration

1.26.3 Syntax Description

This command has no keywords or arguments.

1.26.4 Default

This feature is disabled.

1.26.5 Usage Guidelines

Use the **aaa hint ip-address** command to enable the SmartEdge router to notify the RADIUS server that the IP address in the Framed-IP-Address attribute is the preferred IP address.

This feature applies only to subscribers that you have configured using the *ip address (subscriber)* command (in subscriber configuration mode) with the **pool** keyword. The SmartEdge router selects an unused IP address from the pool and sends it to the RADIUS server in an Access-Request message. The *ip address (subscriber)* command does not apply to subscribers who are configured for SmartEdge router authentication.

The IP address selected from the unnamed IP pool is a hint to the RADIUS server that the selected address is preferred. The RADIUS server can choose to honor the hint or override it with a different IP address. The SmartEdge router uses the address only if the RADIUS server confirms that it is acceptable; the SmartEdge router action corresponding to the RADIUS response is described in the *IP Address Assignment* section.

Note: This command is not available if you have enabled global subscriber authentication using the **aaa global authentication subscriber** command (in global configuration mode).

Use the **no** form of this command to disable this feature.

1.26.6 Examples

The following example shows how to enable this feature in the `customers` context:

```
[local]Redback(config)#context customers
[local]Redback(config-cxt)#aaa hint ip-address
```

1.27 aaa ip-pool allocation first-available

aaa ip-pool allocation first-available

no aaa ip-pool allocation first-available

default fault aaa ip-pool allocation

1.27.1 Purpose

Specifies that the SmartEdge router uses a first-available algorithm to allocate IP addresses to subscribers.

1.27.2 Command Mode

Global configuration

1.27.3 Syntax Description

This command has no keywords or arguments.

1.27.4 Default

The SmartEdge router uses a round-robin algorithm to allocate IP addresses to subscribers.

1.27.5 Usage Guidelines

Use the **aaa ip-pool allocation first-available** command to specify that the SmartEdge router uses a first-available algorithm to allocate IP addresses to subscribers.

When the SmartEdge router receives a request for an IP address, by default it uses the round-robin method to select an address from the IP pool. The round-robin method begins its search where the last search ended; that is, the SmartEdge router checks whether the first address in the IP pool following the last allocated IP address is available. If this address is unavailable, the SmartEdge router checks the next address until either an available address is assigned or the pool is exhausted.

In the first-available method, the search for an available IP address always begins with the first address in the pool.

Use the **no** or **default** form of this command to revert to the default behavior.

1.27.6 Examples

The following example shows how to specify that the SmartEdge router uses a first-available algorithm to allocate subscriber IP addresses:

```
[local]Redback(config)#aaa ip-pool first-available
```

1.28 aaa last-resort

aaa last-resort context *ctx-name* [**append**]

no aaa last-resort

1.28.1 Purpose

Specifies the context in which authentication of a subscriber should be attempted if the subscriber name does not contain a valid domain or context that has been configured in the system.

1.28.2 Command Mode

Global configuration

1.28.3 Syntax Description

context *ctx-name*	Name of the last resort context.
append	Optional. Appends the **@** symbol and context name to the subscriber's name.

1.28.4 Default

No last resort context is configured.

1.28.5 Usage Guidelines

Use the **aaa last-resort** command to specify the context in which authentication of a subscriber name is to be attempted whenever the domain portion of the subscriber name provided cannot be matched to any configured context or domain.

At the time you enter this command, the SmartEdge router does not check to ensure you specify a valid context. When a subscriber attempts to connect, and the SmartEdge router attempts to validate the subscriber in the last resort context, an error message displays if the context does not exist.

Only one last resort context can be in effect at a time. To change the last resort context, create a new one and it overwrites the existing one.

Note: To use Remote Authentication Dial-In User Service (RADIUS), the IP address or hostname of at least one RADIUS server must be configured in the last resort context. To configure the server's IP address or hostname, enter the **radius server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** form of this command to remove the last resort context.

1.28.6 Examples

The following configuration example assumes three contexts: `california`, `nevada`, and `otherstates`. A username, `jill@arizona`, is submitted for authentication, but there is no configured `arizona` context. The following example configures the system in such a way that `jill@arizona` would be submitted for authentication in the `otherstates` context:

```
[local]Redback(config)#aaa last-resort context otherstates
```

1.29 aaa maximum subscriber

aaa maximum subscriber active ***count***

{**no** | **default**} **aaa maximum subscriber**

1.29.1 Purpose

Limits the number of subscriber sessions that can be simultaneously active in a given context.

1.29.2 Command Mode

Context configuration

1.29.3 Syntax Description

active ***count***	Maximum number of subscriber sessions that can be simultaneously active. The value of the ***count*** argument is dependent on the purchased subscriber license, the SmartEdge router platform, and the controller card. Table 1 lists the possible values.

1.29.4 Default

There is no limit to the number of subscriber sessions that can be simultaneously active in a given context.

1.29.5 Usage Guidelines

Use the **aaa maximum subscriber** command to limit the number of subscriber sessions that can be simultaneously active in a given context.

Table 1 lists the values for the **active** ***count*** construct.

Table 1 Context Maximum Subscriber Sessions

SmartEdge Router	Controller Card	Value
SmartEdge 100 router	Controller carrier card	16,000
SmartEdge 400 router	XCRP4	256,000
SmartEdge 600 router	XCRP4	256,000
SmartEdge 800 router	XCRP4	256,000
SmartEdge 1200 router	XCRP4	256,000
SmartEdge 1200H router	XCRP4	256,000

Note: The **subscriber** command (in software license configuration mode) specifies the maximum number of active subscriber sessions.

Use the **no** or **default** form of this command to restore the default of no limit to the number of subscriber sessions.

1.29.6 Examples

The following example shows how to set the maximum number of simultaneous active subscriber sessions for the `local` context to `100`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa maximum subscriber active 100
```

1.30 aaa password

aaa password {**default** ***password*** [**disable-subscriber** | **ipv4-address-release-control**] | **disable-subscriber**}

no aaa password default

1.30.1 Purpose

Changes the default authentication and authorization password for the authentication, authorization, and accounting (AAA) to the specified password.

It also disables the default authentication and authorization password on the subscriber circuits, or sets the password for IPv4 address re-requests to RADIUS when IPv4 address save mode is enabled.

1.30.2 Command Mode

Context configuration

1.30.3 Syntax Description

default *password*	Changes the default authentication and authorization password to the specified password. The password is an alphanumeric string and is plaintext. Control characters are not allowed.
disable-subscriber	Disables the default authentication and authorization password on the subscriber circuits.
ipv4-address-release-control	The password specified is used in IPv4 address save mode for address re-requests. The password can be a maximum of 63 characters.

1.30.4 Default

The default authentication and authorization password is “Redback”.

1.30.5 Usage Guidelines

Use the **aaa password** command to change the default authentication and authorization password for the AAA or disable the default authentication and authorization password on subscriber circuits, or change the password for IPv4 address save mode re-requests. To change the default authentication and authorization password to a specified password, use the **default** keyword with the **aaa password** command. This new default password is saved in the encrypted form. When you enter the show configuration command, the display shows the default AAA password in the encrypted form.

To disable the default authentication and authorization password on subscriber circuits, use the **disable-subscriber** keyword with the **aaa password** command.

To change the password for IPv4 address save mode re-requests, use the **ipv4-address-release-control** keyword with the **aaa password** command.

Use the **no** form of this command to restore the default password of “Redback”.

1.30.6 Examples

The following example configures the new default AAA password of secret123:

```
[local]Redback(config-ctx)#aaa password default secret123
```

The following example configures the new default AAA password of secret123 and disable this default AAA password on the subscriber circuits:

```
[local]Redback(config-ctx)#aaa password default secret123
disable-subscriber
```

The following example configures the new default password of **secret123** for IPv4 address save mode re-requests:

```
[local]Redback(config-ctx)#aaa password default secret123
ipv4-address-release-control
```

1.31 aaa provision binding-order

aaa provision binding-order ip-address-attr l2tp-attr

no aaa provision binding-order ip-address-attr l2tp-attr

1.31.1 Purpose

Changes the default order in which the SmartEdge router searches for the Remote Authentication Dial-In User Service (RADIUS) and Layer 2 Tunneling Protocol (L2TP) attributes to find the IP address be used to bind a subscriber circuit.

1.31.2 Command Mode

Context configuration

1.31.3 Syntax Description

ip-address-attr	Uses the IP address in the Framed-IP-Address attribute in the authentication message received from a RADIUS server.
l2tp-attr	Uses the IP address in the Sub-Address attribute value pair (AVP) in the incoming call request (ICRQ) message received from the L2TP access concentrator (LAC) peer.

1.31.4 Default

The SmartEdge router searches for the L2TP attribute before searching for the RADIUS attribute.

1.31.5 Usage Guidelines

Use the **aaa provision binding-order** command to change the default order in which the SmartEdge router searches for the RADIUS and L2TP attributes to find the IP address to be used to bind a subscriber circuit. The circuit binding has been created using the **bind authentication** command (in the circuit's configuration mode).

Use this command to enable the SmartEdge router to look for the RADIUS Framed-IP-Address attribute before looking at the L2TP Sub-Address AVP. If the Framed-IP-Address attribute does not exist, the L2TP ICRQ message is examined for the Sub-Address AVP. If the Sub-Address AVP does not exist, the session is not brought up.

Use the **no** form of this command to specify the default order.

For more information about using the **bind authentication** command to create a dynamic binding, see *Configuring Bindings*.

1.31.6 Examples

The following example shows how to specify that the IP address (and its interface) in the RADIUS record be used to bind a subscriber circuit:

```
[local]Redback(config-ctx)#aaa provision binding-order ip-address-attr
l2tp-attr
```

1.32 aaa provision route

aaa provision route ip-netmask encapsulation ***encaps-type*** **[use-framed-route]**

{**no** | **default**} **aaa provision route ip-netmask [use-framed-route]**

1.32.1 Purpose

Enables the SmartEdge router to assign one or a range of IP addresses specified by the subscriber IP netmask in the RADIUS Framed-IP-Netmask attribute to a PPP or PPPoE subscriber. This command also installs the IP netmask as a subnet route for the subscriber in the route table.

1.32.2 Command Mode

Context configuration

1.32.3 Syntax Description

ip-netmask	Installs the subscriber ip-netmask as subnet route in the route table.
encapsulation *encaps-type*	Encapsulation type, according to one of the following keywords: • **ppp**—Specifies Point-to-Point Protocol (PPP)-encapsulated subscriber circuits. • **pppoe**—Specifies PPP over Ethernet (PPPoE)-encapsulated subscriber circuits. • **ppp pppoe**—Specifies PPP- and PPPoE-encapsulated subscriber circuits.
use-framed-route	Assigns one ip address specified within the IP of the subscriber IP netmask to the PPP or PPPoE subscriber. This keyword also installs the IP netmask as subnet route in the route table for the entire address space specified in the IP netmask.

1.32.4 Default

The Framed-IP-Netmask attribute is ignored.

1.32.5 Usage Guidelines

Use the **aaa provision route** command to enable the SmartEdge router to assign one or a range of IP addresses specified by the subscriber IP netmask in the RADIUS Framed-IP-Netmask attribute to a PPP or PPPoE subscriber. This command also installs the IP netmask as a subnet route for the subscriber in the route table.

If you configure the **use-framed-route** keyword with the **aaa provision route** command, the subscriber is assigned one IP address specified in the Framed-IP-Netmask attribute. Otherwise, the entire range of addresses specified by IP netmask is assigned to the subscriber.

Note: The SmartEdge router currently can assign up to an entire Class C address to subscribers. If the IP netmask in the Framed-IP-Netmask attribute is greater than a Class C address, use the **use-framed-route** keyword. This keyword allows the operating system to support subscribers that have Class B network behind them.

Use the **no** or **default** form of this command to revert to the default behavior.

1.32.6 Examples

The following example shows how to enable a direct connection to PPP routers:

```
[local]Redback(config)#context remote
[local]Redback(config-ctx)#aaa provision route ip-netmask encapsulation ppp
```

The following example shows how to enable a direct connection to a PPPoE router with a Class B network behind it:

```
[local]Redback(config)#context abcremote
[local]Redback(config-ctx)#aaa provision route ip-netmask encapsulation pppoe use-framed-route
```

1.33 aaa rate-report-factor

aaa rate-report-factor {**adsl1**| **adsl2** | **adsl2+** | **vdsl1** | **vdsl2** | **sdsl** | **unknown**} *percentage*

no aaa rate-report-factor

1.33.1 Purpose

Multiplies the raw digital subscriber line (DSL) data rate by a factor and reports the result for one or more line types as the subscriber traffic rate in Remote Authentication Dial-In User Service (RADIUS) and Layer 2 Tunneling Protocol (L2TP) messages.

1.33.2 Command Mode

Context configuration

1.33.3 Syntax Description

adsl1	Specifies an asymmetric DSL line type.
adsl2	Specifies an asymmetric DSL line type.
adsl2+	Specifies an asymmetric DSL line type.
vdsl1	Specifies a very high DSL line type.
vdsl2	Specifies a very high DSL line type.
sdsl	Specifies an asymmetric DSL line type.

unknown	Specifies an unknown DSL line type.
percentage	Factor by which you want to multiply the data rate prior to sending the RADIUS message.

1.33.4 Default

No rate adjustment is calculated for any DSL line type.

1.33.5 Usage Guidelines

Use the **aaa rate-report-factor** command to multiply the raw DSL data rate by a factor and report the result for one or more line types as the subscriber traffic rate in RADIUS and L2TP messages.

Access nodes send raw data rates of one or more DSL line types to the SmartEdge router; however, only a portion of the raw data rate is available for subscriber traffic. You can configure the SmartEdge router to multiply the raw data rate for each type of DSL line by a specific percentage.

The magnitude of the adjustment can differ by DSL line type. For this reason, you can specify a different factor for each possible line type. You must issue this command once for each line type that you expect connected access nodes to use.

The SmartEdge router sends the adjusted rate in RADIUS vendor-specific attribute (VSA) 185, DSL_Actual_Rate_Down_Factor and L2TP (Tx) Connect Speed attribute-value pair (AVP) 24 attributes. If you do not specify a factor for a specific line type, an unaltered learned rate for that line type is sent in the attributes.

Note: This command adjusts only the reported rates for the mentioned attributes. It does not affect data rates used for traffic shaping or quality of service (QoS) policies. QoS policies use the raw rates combined with more precise encapsulation information to achieve proper metering and shaping.

Use the **no** form of this command to revert to the default behavior.

1.33.6 Examples

The following example shows how to enable the SmartEdge router to multiply the DSL line type data rate for ADSL1 by 80% prior to sending a RADIUS accounting message:

```
[local]Redback(config-ctx)#aaa rate-report-factor adsl1 80
```

1.34 aaa reauthorization bulk

aaa reauthorization bulk {**global** | **none** | **radius**}

{**no** | **default**} **aaa reauthorization bulk**

1.34.1 Purpose

Configures subscriber reauthorization so that attribute changes can be dynamically applied to active subscriber sessions, without requiring Point-to-Point Protocol (PPP) renegotiation and without interrupting or dropping active sessions.

1.34.2 Command Mode

Context configuration

1.34.3 Syntax Description

global	Enables reauthorization of all subscribers in the current context through one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the local context.
none	Disables subscriber reauthorization.
radius	Enables reauthorization of subscribers in the current context through one or more RADIUS servers with IP addresses or hostnames in the same context.

1.34.4 Default

None

1.34.5 Usage Guidelines

Use the **aaa reauthorization bulk** command to configure subscriber reauthorization so that attribute changes can be dynamically applied to active subscriber sessions, without requiring PPP renegotiation and without interrupting or dropping active sessions. After this command has been enabled, enter the **reauthorize** command (in exec mode) to initiate subscriber reauthorization.

The standard RADIUS attributes and Redback VSAs that are supported with dynamic subscriber reauthorization are listed in *RADIUS Attributes*.

Note: The SmartEdge router appends the context name to the subscriber name when sending reauthorization messages; for example, `joe@local`.

Note: You must configure at least one RADIUS server in the local or the current context before any messages can be sent to it. To configure the server, enter the **`radius server`** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Note: To enable RADIUS authentication, you must enter the **`aaa authentication subscriber`** command (in context configuration mode).

Use the **`no`** or **`default`** form of this command to disable dynamic subscriber reauthorization.

1.34.6 Examples

The following example shows how to enable the global reauthorization of all subscribers in the SmartEdge router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa reauthorization bulk global
```

The following is an example of a subscriber record on a RADIUS server. The subscriber has requested a new service that is translated to a particular session `timeout` value:

```
#reauth of absolute timeout
reauth-501@local User-Password==”redback”
    Service-Type=Outbound-User,
    Reauth_String=”2;pppoe1@local;27;1000;”
```

Before the administrator enters the **`reauthorize`** command (in exec mode), the subscriber record appears as:

```
[local]Redback>show subscribers active


pppoe1@local
    Circuit 13/1 vpi-vci 0 33
    Internal Circuit 13/1:1023:63/1/2/22
    Current port-limit unlimited
    ip address 10.1.1.4
```

In the following example, the administrator enters the **`reauthorize`** command (in exec mode) and the subscriber session is reauthorized with the new `timeout` attribute added:

```
[local]Redback>reauthorize username pppoe1@local
[local]Redback>show subscribers active


pppoe1@local
    Circuit 13/1 vpi-vci 0 33
    Internal Circuit 13/1:1023:63/1/2/22
    Current port-limit unlimited
    ip address 10.1.1.4
    timeout absolute 1000
```

1.35 aaa route-download

aaa route-download radius [**username-prefix** *prefix*] | [**password** *password*] | [**sync-time** *hh:mm:ss*] | [**interval** *interval*] | [**default-cost** *cost*]

aaa route-download global

no aaa route-download

1.35.1 Purpose

Enables AAA route download on the SmartEdge router. The route-download functionality is disabled by default. The mandatory parameter radius or global specifies the route-download method.

1.35.2 Command Mode

Context configuration

1.35.3 Syntax Description

radius	Uses RADIUS as the route download method.
username-prefix *prefix*	The user to be specified in the authentication request to the server. The default is the hostname configured for the SmartEdge router.
password *password*	The password to be used to authenticate the specified username via RADIUS.
sync-time *hh:mm:ss*	A time of day, in 24-hour notation, at which route download requests should be automatically sent to the route download server. If not specified, automatic downloads are not initiated.

interval *interval*	The interval, in minutes, after which download is to be re-initiated, as measured since the time of the last download. The range is 60 to 1440. The default is 720 minutes.
default-cost *cost*	The routing metric to be applied to all routes downloaded in this way. The range is 0 to 255. The default is 0. If the metric is specified in the command and also within the RADIUS Framed-Route attribute, the cost defined in RADIUS takes precedence.
global	Uses global route-download method. This method does not require other parameters.

1.35.4 Default

The default interval is 720 minutes. The default cost is 0.

1.35.5 Examples

Use the following command to configure route download using the radius method, with default parameters:

```
[local]Redback(config-ctx)#aaa route-download radius
```

1.36 aaa session rate-limit

aaa session rate-limit [**access-accept**] [**access-reject**] *count* **interval** *count-interval* **drop-ipcp-interval** *drop-interval*

no aaa session rate-limit [**access-accept**] [**access-reject**] *count* **interval** *count-interval* **drop-ipcp-interval** *drop-interval*

1.36.1 Purpose

Prevents SmartEdge from sending too many Access Request packets to RADIUS and causing denial of service (DoS) due to receiving too many Access Accepts or Access Rejects from RADIUS.

1.36.2 Command Mode

Context configuration

1.36.3 Syntax Description

access-accept	Count Access Accept packets received from RADIUS in the specified interval.
access-reject	Count Access Reject packets received from RADIUS in the specified interval.
count	The maximum number of Access Accept packets or Access Reject packets that can be received from RADIUS within the specified interval before further IPCP Configuration Requests will be dropped. The initial Access Accept or Access Reject does not count toward this threshold.
interval ***count-interval***	The interval over which to count Access Accept or Access Reject packets. The range is 1 to 127 seconds.
drop-ipcp -interval ***drop-interval***	The interval over which to drop IPCP Configuration Requests when the threshold is reached. If IPCP Configuration Requests are dropped, the SmartEdge does not send Access Requests to RADIUS. The range is 1 to 127 seconds.

1.36.4 Default

No limits are placed on the number of Access Request packets that can be sent to RADIUS.

1.36.5 Usage Guidelines

Use the **aaa session rate-limit** command to limit the number of Access Request packets sent to RADIUS based on the number of Access Accept or Access Reject packets received from RADIUS over the specified interval. When the threshold is reached, SmartEdge drops all IPCP Configuration Requests received from the customer for a specified drop interval. When IPCP Configuration Requests are dropped, Access Requests are not being sent to RADIUS.

This command can prevent DoS when the SmartEdge is receiving too many Access Accepts or Access Rejects from RADIUS.

Use the **no** form of this command to allow unlimited Access Request packets to be sent to RADIUS.

1.36.6 Examples

The following example specifies that if 100 Access Accept packets or 100 Access Reject packets are received from RADIUS within a 30-second interval, drop all IPCP Configuration Requests received from the customer for 20 seconds:

```
[local]Redback(config-ctx)#aaa session rate-limit access-accept
access-reject 100 interval 30 drop-ipcp-interval 20
```

1.37 aaa update subscriber

aaa update subscriber *interval*

{**no** | **default**} **aaa update subscriber**

1.37.1 Purpose

Sends updated accounting records for subscriber sessions in the current context to one or more Remote Authentication Dial-In User Service (RADIUS) servers with IP addresses or hostnames configured in the same context.

1.37.2 Command Mode

Context configuration

1.37.3 Syntax Description

interval	Period (in minutes) between accounting updates. The range of values is 10 to 10,080.

1.37.4 Default

Updates for subscriber accounts are not performed.

1.37.5 Usage Guidelines

Use the **aaa update subscriber** command to send updated accounting records for subscriber sessions in the current context to one or more RADIUS servers with IP addresses or hostnames configured in the same context.

Note: You must configure accounting using the **aaa accounting subscriber** command (in context configuration mode) with the **radius** keyword.

Note: To use RADIUS, the IP address or hostname of at least one RADIUS accounting server must be configured in the context to which the subscriber is to be bound. To configure the server's IP address or hostname, enter the **radius accounting server** command (in context configuration mode); for more information, see *Configuring RADIUS*.

Use the **no** or **default** form of this command to disable subscriber account updating.

1.37.6 Examples

The following example shows how to configure an update to be sent every 20 minutes, for as long as the subscriber session lasts:

```
[local]Redback(config-ctx)#aaa update subscriber 20
```

1.38 aaa username-format

aaa username-format {**domain** | **username**} ***separator*** **[rightmost-separator]**

no aaa username-format {**domain** | **username**} ***separator*** **[rightmost-separator]**

1.38.1 Purpose

Defines one or more schemas for matching the format of structured usernames.

1.38.2 Command Mode

Global configuration

1.38.3 Syntax Description

domain	Specifies that the domain portion of the structured username is to precede the user portion.
username	Specifies that the user portion of the structured username is to precede the domain portion.

separator	Character that separates the user portion of the structured username from the domain portion. The possible characters are %, -, @, _, \\, #, and /. To designate a backslash (\), you must enter it on the command line as two backslashes (\\). A single backslash has a reserved meaning in the SmartEdge router. A maximum of six characters can be used in a single schema.
rightmost-separator	Specifies that the far right (rightmost) character within a structured username that contains multiple separators is to be treated as the separator character.

1.38.4 Default

If no username formats are specified with this command, the SmartEdge router default format of ***username@domain-name*** is checked for a format match.

1.38.5 Usage Guidelines

Use the **aaa username-format** command to define one or more schemas for matching the format of structured usernames. A username can be for a subscriber or an administrator.

You can use this command multiple times to create a list of formats against which an incoming username is matched. The first format configured is checked first for a match, then the second, and so on until a match is found or until the configured username formats are exhausted.

Use the **rightmost-separator** keyword with the **aaa username-format** command when you have multiple separators within a structured username; for example, joe@gold@example.com. If the **rightmost-separator** keyword is configured, the SmartEdge router treats the far right (rightmost) separator character as the separator that divides the user portion of the structured username from the domain portion.

If no username formats are explicitly defined with the **aaa username-format** command, the SmartEdge router checks the default format of username@domain-name for a match.

Use the **no** form of this command to remove the specified format from those considered to be valid structured-username formats.

1.38.6 Examples

The following example shows how to configure a structured-username format with the subscriber name specified first, separated from its domain by the % symbol:

```
[local]Redback(config)#aaa username-format username %
```

In this example, for a subscriber, `joe`, configured in the `local` context, the SmartEdge router checks for a match against the structured-username `joe%local`.

The following example shows how to configure a structured-username format with the domain name specified first, separated from the subscriber name by the `/` symbol:

```
[local]Redback(config)#aaa username-format domain /
```

In this example, for a subscriber, `joe`, configured in the `local` context, the SmartEdge router checks for a match against the format `local/joe`.

The following example shows how to configure a structured-username format with the domain name specified first, separated from the subscriber name using the far right (rightmost) separator, a `@` symbol:

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

In this example, for a username, `local@example.com@joe`, the SmartEdge router checks for the far right separator, a `@` symbol. For this username, the subscriber name is `joe` and the context is `local@example.com`.

1.39 abort

`abort`

1.39.1 Purpose

Deletes an outstanding database transaction.

1.39.2 Command Mode

All configuration modes

1.39.3 Syntax Description

This command has no keywords or arguments.

1.39.4 Default

None

1.39.5 Usage Guidelines

Use the **abort** command to delete an outstanding database transaction, which includes all configuration commands entered since the beginning of the configuration session, or since the latest **abort** or **commit** command.

In any configuration mode, this command deletes the database transaction for the current configuration session; a new database transaction is started for the configuration session, and subsequent commands entered in the session are part of the new transaction.

Caution!

Risk of data loss. When you use the **abort** command (in any configuration mode) to delete the current transaction, all configuration information associated with the transaction is deleted and cannot be recovered. To minimize the risk, save your configuration before and after you enter the transaction commands, and do not abort the transaction without ensuring that you do not need the commands in it.

1.39.6 Examples

The following example shows how to delete the current database transaction:

```
[local]Redback#abort
```

1.40 absolute

absolute start *yyyy*:*mm*:*dd*:*hh*:*mm* **end** *yyyy*:*mm*:*dd*:*hh*:*mm* [:*ss*] {{**permit** | **deny**} | **class** *class-name*}

no absolute start *yyyy*:*mm*:*dd*:*hh*:*mm* **end** *yyyy*:*mm*:*dd*:*hh*:*mm*

1.40.1 Purpose

Creates an absolute time access control list (ACL) condition statement.

1.40.2 Command Mode

ACL condition configuration

1.40.3 Syntax Description

start *yyyy*:*mm*:*dd*:*hh*:*mm* [:*ss*]	Date and time to start the ACL condition. Arguments are defined as follows: • *yyyy*—Year. • *mm*—Month. The range of values is 1 to 12. • *dd*—Day. The range of values is 1 to 31. • *hh*—Hour in 24-hour format. The range of values is 0 to 23. • *mm*—Minutes. The range of values is 0 to 59. • *ss*—Seconds. Optional. The range of values is 0 to 60.
end *yyyy*:*mm*:*dd*:*hh*:*mm* [:*ss*]	Date and time to stop the ACL condition. Arguments are defined as follows: • *yyyy*—Year. • *mm*—Month. The range of values is 1 to 12. • *dd*—Day. The range of values is 1 to 31. • *hh*—Hour 24-hour format. The range of values is 0 to 23. • *mm*—Minutes. The range of values is 0 to 59. • *ss*—Seconds. Optional. The range of values is 0 to 60.
permit	Applies a permit action to packets processed during the specified time range.
deny	Applies a deny action to packets processed during the specified time range. Used only with IP ACLs.
class *class-name*	Name of the class assigned to policy ACL statements that reference the ACL condition. Used only with policy ACLs.

1.40.4 Default

No ACL condition statements are configured.

1.40.5 Usage Guidelines

Use the **absolute** command to create an absolute time ACL condition statement that, when referenced in an IP ACL statement, permits or denies packets, based on specific date and time ranges. Use this command to create an absolute time ACL conditional statement that, when referenced in a policy ACL statement, assigns a class name to packets.

Use the **no** form of this command to delete the absolute time ACL condition statement.

1.40.6 Examples

The following example shows how to create an absolute time ACL condition statement for the ACL condition `500`, which is referenced in the policy ACL, `policy-acl-forward`. The absolute time ACL condition applies the `Bar003` class name to all policy ACL statements that reference the ACL condition during the time interval beginning on December 15, 2003 at 9:00 p.m. (`21:00`) and ending on the same day at 11:00 p.m. (`23:00`):

```
[local]Redback(config-ctx)#policy access-list policy-acl-forward
[local]Redback(config-access-list)#condition 500 time-range
[local]Redback(config-acl-condition)#absolute start 2003:12:15:21:00 end
2003:12:15:23:00 class Bar003
```

1.41 accept filter prefix-list

accept filter prefix-list

no accept filter prefix-list

1.41.1 Purpose

Advertises to a Border Gateway Protocol (BGP) peer that a BGP speaker can accept address prefix-based route filtering from a peer.

1.41.2 Command Mode

BGP neighbor configuration

1.41.3 Syntax Description

This command has no keywords or arguments.

1.41.4 Default

The command is disabled.

1.41.5 Usage Guidelines

Use the **accept filter prefix-list** command to advertise to a BGP peer that a BGP speaker can accept address prefix-based route filtering from a peer. Use this command to save resources and avoid the generation, transmission, and processing of unnecessary routing updates.

When this command is enabled, and if the BGP peer advertises its preference to send address prefixed-based filtering (through the **send filter prefix-list** command in BGP neighbor configuration mode), the remote peer sends its inbound address prefix-based filtering to the local BGP speaker. The local BGP speaker uses the received address prefix-based filtering along with its local routing policies to determine whether routes should be advertised to the peer.

Note: This command cannot be enabled on a BGP neighbor that is part of a peer group because this feature cannot be customized for individual members inside of a peer group.

Use the **show bgp neighbor** *ip-address* **received prefix-filter** command to display address prefix-based route filtering configuration information.

Use the **no** form of this command to disable a BGP speaker from accepting route filtering from a peer.

For further information, see the Internet Drafts, *Cooperative Route Filtering Capability for BGP-4*, draft-ietf-idr-route-filter-03.txt, and *Address Prefix Based Outbound Route Filter for BGP-4*, draft-chen-bgp-prefix-orf-02.txt.

1.41.6 Examples

The following example shows how to enable the SmartEdge router to accept address prefix-based route filtering from the BGP peer at IP address `10.1.1.1`:

```
[local]Redback(config-bgp)#neighbor 10.1.1.1 external
[local]Redback(config-bgp-neighbor)#accept filter prefix-list
```

1.42 accept-lifetime

accept-lifetime *start-datetime* [{**duration** *seconds* | **infinite** | *stop-datetime*}]

no accept-lifetime ***start-datetime*** [{**duration** ***seconds*** | **infinite** | ***stop-datetime***}]

1.42.1 Purpose

Establishes a start date and time for accepting the key, and optionally, a stop time for accepting the key.

1.42.2 Command Mode

Key chain configuration

1.42.3 Syntax Description

start-datetime	Date and time to start accepting the key being configured. Must be in the format ***yyyy*****:*****mm*****:*****dd*****:*****hh*****:*****mm***[**:*****ss***]. For more information about the format of this argument, see the Usage Guidelines section.
duration ***seconds***	Optional. Number of seconds to continue accepting the key. The range of values is 1 to 2,147,483,646.
infinite	Optional. Specifies that the key is to be accepted indefinitely.
stop-datetime	Optional. Date and time to stop accepting the key being configured. Must be in the format ***yyyy*****:*****mm*****:*****dd*****:*****hh*****:*****mm***[**:*****ss***]. For more information about the format of this argument, see the Usage Guidelines section.

1.42.4 Default

If you do not issue this command, the key is accepted starting immediately and continues to be accepted indefinitely. If you do not specify a duration when issuing this command, the key is accepted indefinitely.

1.42.5 Usage Guidelines

Use the **accept-lifetime** command to specify when the key being configured is to be accepted. The format of the ***start-datetime*** and ***stop-datetime*** arguments is ***yyyy*****:*****mm*****:*****dd*****:*****hh*****:*****mm***[**:*****ss***] and is defined as follows:

- ***yyyy*** = The year in four digits (for example, 2003).
- ***mm*** = The month of the year in two digits (for example, 01). The range of values is 1 to 12.

- ***dd*** = The day of the month in two digits (for example, 24). The range of values is 1 to 31.
- ***hh*** = The hour of the day in two digits (for example, 23). The range of values is 0 to 23.
- ***mm*** = The minute of the hour in two digits (for example, 59). The range of values is 0 to 59.
- ***ss*** = Optional. The second of the minute in two digits (for example, 55). The range of values is 0 to 59.

If you issue the **accept-lifetime** command without any optional constructs, the key is accepted starting with the date and time that you specify and continues to be accepted indefinitely. You can replace an existing accept lifetime value by issuing the **accept-lifetime** command again and specifying new values.

Use the **no** form of this command to specify that the key is no longer to be accepted.

1.42.6 Examples

The following example shows how to establish a lifetime acceptance of January 25, 2002 at one minute and one second after 4:00 a.m. The key continues to be accepted indefinitely:

```
[local]Redback(config-key-chain)#accept-lifetime 2002:01:25:04:01:01
```

The following example shows how to establish a lifetime acceptance of January 25, 2002 at exactly midnight, and specify that the key is to be accepted for 30 minutes (1800 seconds):

```
[local]Redback(config-key-chain)#accept-lifetime 2002:01
:25:00:00 duration 1800
```

1.43 access-group

access-group [***acl-name***]

no access-group [***acl-name***]

1.43.1 Purpose

Applies a policy access control list (ACL) to a class-based Network Address Translation (NAT) policy and enters policy group configuration mode. This command is used for referencing IPv4 ACLs only.

1.43.2 Command Mode

NAT policy configuration

1.43.3 Syntax Description

acl-name	Optional. Name of the policy ACL created using the **policy access-list** command (in context configuration mode); required to apply or remove a static policy ACL.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **access-group** command to apply a policy ACL to a class-based NAT policy and enter policy group configuration mode.

If the class-based policy is defined as RADIUS-guided, the policy ACL that it references can be dynamic, static, or both:

- A dynamic policy ACL is one that the SmartEdge router applies to the class-based policy for a particular subscriber session using the rules specified in an instance of vendor-specific attribute (VSA) 164 that the RADIUS server supplies in an access-response or COA message for the subscriber.
- A static policy ACL is a locally configured policy access list; its name must be explicitly specified.

You can apply both a dynamic policy ACL and a static policy ACL. If VSA 164 is used to apply the dynamic ACL, the static policy ACL takes precedence; locally configured access list rules are evaluated before those from a dynamic ACL specified through VSA 164.

If the class-based policy is not defined as RADIUS-guided, the policy ACL that it references must be static, and the **access-group** command must specify the locally configured access list name.

Note: The names of the IP and policy ACLs in the output of the **show access-group** command (in any mode) include the prefix “ADF” for dynamic IP ACLs and “DPF” for dynamic policy ACLs.

Use the **no** form of this command to remove a static policy ACL from a specified policy.

To remove a policy ACL from a RADIUS-guided policy, you must delete the RADIUS-guided policy and then re-create it.

1.43.6 Examples

The following example shows how to apply the `nat-acl` policy ACL to the `nat-policy` NAT policy. The `nat-acl` ACL defines two classes—`nat-pool` and `ignore`:

```
[local]Redback(config)#context nat
[local]Redback(config-ctx)#nat policy nat-policy

[local]Redback(config-policy-nat)##access-group nat-acl

[local]Redback(config-policy-acl)#class pool

[local]Redback(config-policy-acl-class)#pool nat-pool local
[local]Redback(config-policy-acl-class)#class ignore
[local]Redback(config-policy-acl-class)#ignore
[local]Redback(config-policy-acl-class)#
```

1.44 access-group (IGMP snooping profile configuration mode)

access-group ***acg-name***

no access-group*acg-name*

1.44.1 Purpose

Configures an IGMP profile to filter IGMP control messages that are received by an associated bridge so that nonmatching packets are not processed.

1.44.2 Command Mode

IGMP snooping profile configuration

1.44.3 Syntax Description

acg-name	Access group whose messages you want to filter.

1.44.4 Default

IGMP control message filtering is disabled, and every incoming packet is processed.

1.44.5 Usage Guidelines

Use the **access-group** command to filter IGMP control messages that are received by an associated bridge so that nonmatching packets are not processed.

Used in *Configuring IP Multicast*.

Use the **no** form of this command to disable IGMP control message filtering.

1.44.6 Examples

The following example shows how to configure IGMP message filtering in the sanjose1 IGMP snooping profile. Bridges that reference the sanjose1 IGMP profile filter received IGMP messages:

```
[local]Redback #configure
[local]Redback(config)#igmp snooping profile sanjose1
[local]Redback(config-igmp-snooping-profile)# access-group acl1
```

1.45 access-list

[no] access-list {**count** *counter-type* {**ip** | **ipv6** | **policy** | **ipv6-policy**} | **log ip**}

1.45.1 Command Mode

Subscriber configuration

1.45.2 Syntax Description

count *counter-type*	ACL counter type, according to one or more of the following keywords: • **ip**—Keep count for IP ACLs. • **policy**—Keep count for policy ACLs. • **ipv6**—Keep count for IPv6 ACLs. • **ipv6-policy**—Keep count for IPv6 policy ACLs
log ip	Enables logging of dropped counters for IPv4 ACLs.

1.45.3 Default

ACL counters are not enabled for any subscriber records or profiles, or the default subscriber.

1.45.4 Usage Guidelines

Use the **access-list** command to enable access control-list (ACL) counters or logging for the default subscriber profile, a named subscriber profile, or a named subscriber record.

Use the **no** form of this command to disable ACL counters for the default subscriber profile, a named subscriber profile, or a named subscriber record.

1.45.5 Examples

The following example shows how to enable ACL IP counters for the default subscriber profile:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#access-list count ip
```

1.46 access-line access-node-id

access-line access-node-id *ani* **slotport** *slot*/*port*

no access-line

1.46.1 Purpose

Specifies the agent circuit ID that the system uses to match an incoming Access Node Control Protocol (ANCP) message to a digital subscriber line (DSL).

1.46.2 Command Mode

dot1q PVC configuration

1.46.3 Syntax Description

ani	Access node identifier (ANI). Alphanumeric string. Enclose the string in double quotes (“).
slotport *slot*/*port*	Slot and port of the DSL access multiplexer (DSLAM). This string must not include any spaces. Enclose the string in double quotes (“).

1.46.4 Default

No agent circuit ID is specified for the circuit.

1.46.5 Usage Guidelines

Use the **access-line access-node-id** command to specify the agent circuit ID that the system uses to match an incoming ANCP message to a DSL. This command identifies a unique configured agent circuit ID to be associated with an 802.1Q PVC or 802.1Q tunnel. The data contained in the message is applied to the circuit that matches the specified agent circuit ID. The agent circuit ID received from the DSLAM is either unformatted (a “blind string”) or it can conform to one of the formats specified in `DSL Forum Specification TR-101, R-124`, as follows:

- For ATM DSLs—ANI atm ***slot/port:vpi.vci***
- For Ethernet DSLs—ANI eth slot/port[:vlan-id]

In the formatted version, the ***ANI*** field is always a blind string that identifies the DSLAM ANI; the SmartEdge router stores but does not process this string; it only searches for a space that terminates the string. The slot/port field is also a blind string; the SmartEdge router searches for a colon (:) that terminates the field, discards the colon and the remaining text, and stores the remaining string.

Use the ***ani*** argument to specify the DSLAM ANI portion of the agent circuit ID to which the incoming DSLAM ANIs are matched; use the slotport slot/port construct to specify the DSLAM slot and port. To match incoming agent circuit IDs, duplicate the incoming format used by the DSLAM.

The total number of characters in the values for the ***ani*** and ***slotport*** fields must be fewer than 63.

Use the **no** form of this command to specify the default condition.

The following examples of incoming DSLAM messages do not match; the reason is provided:

Table 2 DSLAM Message Mismatches

`10.101.90.4/0.0.0.0 foo 3/2:bar`	Invalid line type “foo”
`10.101.90.4/0.0.0.0 atmxx 3/2:2.3`	Invalid line type “atmxx”
`10.101.90.4/0.0.0.0atm 3/2:2.3`	No space before “atm”
`10.101.90.4/0.0.0.0-atm 3/2:2.3`	“-” instead of space before “atm”
`10.101.90.4/0.0.0.0 atm 3/2#2.3`	# instead of colon after the port
`10.101.90.4/0.0.0.0 atm 3/2 2.3`	Space instead of colon after the port
`10.101.90.4/0.0.0.0 atm 3/22`	Wrong port number

1.46.6 Examples

The following example shows how to specify an agent circuit ID to which incoming DSLAM messages are matched:

```
[local]Redback(config-dot1q-pvc)#dot1q pvc 1:1 encapsulation pppoe
[local]Redback(config-dot1q-pvc)#access-line access-node-id
"10.101.90.4/0.0.0.0" slotport "3/2"
```

The following examples of incoming DSLAM messages match:

```
10.101.90.4/0.0.0.0 atm 3/2:2.3
10.101.90.4/0.0.0.0 eth 3/2:7
```

The following example specifies the agent circuit ID for the circuit tagged as `pvc 200` with the profile `pwfq`. The PVC is a tunnel indicated by the specification of **`encapsulation 1qtunnel`** keywords with the **`doct1q pvc`** command:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-dot1q-pvc)#dot1q pvc 200 profile pwfq encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#access-line access-node-id
"10.101.80.3/0.0.0.0" slotport "3/2"
```

1.47 access-line adjust

`access-line adjust` {**`cvlan`** | **`subscriber`**}

`no access-line adjust` {**`cvlan`** | **`subscriber`**}

1.47.1 Purpose

Overrides the rates specified by the quality of service (QoS) policies attached to this subscriber record, named profile, or the default profile with the rates learned from the digital subscriber line (DSL) access multiplexer (DSLAM).

1.47.2 Command Mode

Subscriber configuration

1.47.3 Syntax Description

cvlan	Applies the rate learned from the DSLAM to the port, 802.1Q tunnel, or 802.1Q permanent virtual circuit (PVC) to which the QoS policy is attached.
subscriber	Applies rate information learned from the DSLAM to the subscriber circuit. This is the default.

1.47.4 Default

The rate learned from the DSLAM is applied to the subscriber circuit.

1.47.5 Usage Guidelines

Use the **access-line adjust** command to override the rates specified by the QoS policies attached to this subscriber record, named profile, or the default profile with the rates learned from the DSLAM. The system applies the DSLAM rate.

Use the **no** form of this command to specify the default condition.

1.47.6 Examples

The following example shows how to override the rate specified by any QoS policy attached to the `default` subscriber profile:

```
[local]Redback(config)#context isp2
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#access-line adjust subscriber
```

1.48 access-line agent-circuit-id

access-line agent-circuit-id ***string***

no access-line agent-circuit-id ***string***

1.48.1 Purpose

Specifies the agent circuit ID that the system uses to match an incoming ANCP message to a circuit.

1.48.2 Command Mode

dot1q PVC configuration

1.48.3 Syntax Description

string Agent circuit ID. A text string with up to 63 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces.

1.48.4 Default

No agent circuit ID is specified for a DSL on this circuit. The SmartEdge router can learn this information from a Point-to-Point Protocol (PPP) over Ethernet (PPPoE) tag or a Dynamic Host Control Protocol (DHCP) option 82 tag.

1.48.5 Usage Guidelines

Use the **access-line agent-circuit-id** command to specify the agent circuit ID that the system uses to match an ANCP message to a circuit, which can be either an 802.1Q PVC or 802.1Q tunnel. An incoming ANCP message contains an agent circuit ID. The data contained in this message is applied to the circuit that matches that agent circuit ID. The agent circuit ID received from the DSL access multiplexer (DSLAM) must match the text string exactly.

If the value learned from a subscriber session on this DSL differs from the configured value for the ***string*** argument, the system generates an error log message and uses the configured value.

Note: For a more flexible approach to matching an ANCP message to a circuit, use the **access-line access-node-id** command (in dot1q PVC configuration mode).

Use the **no** form of this command to specify the default condition.

1.48.6 Examples

The following example shows how to specify the agent circuit ID for all subscriber sessions:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 100
[local]Redback(config-dot1q-pvc)#access-line agent-circuit-id
"dslam-10.1.1.1 dot1q 2/1:1:1"
```

The following example shows how to specify the agent circuit ID for the circuit tagged as `pvc 100` with the profile `pwfq`. The PVC is a tunnel indicated by the specification of **encapsulation 1qtunnel:**

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 100 profile pwfq encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#access-line agent-circuit-id
"10.2.1.1 eth 3/1:100"
```

1.49 access-line rate

access-line rate {**in** | **out** [**metering** | **queuing**]} [**ancp**]

no access-line rate {**in** |**out**}

1.49.1 Purpose

Overrides the rates specified by the quality of service (QoS) policies attached to subscriber session or 802.1q VLAN with the rates learned from the neighbor peer (DSLAM) through Access Node Control Protocol (ANCP) or Point-to-Point Protocol over Ethernet (PPPoE), Point-to-Point Protocol over ATM (PPPoA), or Dynamic Host Configuration Protocol (DHCP) TR-101 tags.

1.49.2 Command Mode

- Subscriber configuration
- dot1q profile configuration

1.49.3 Syntax Description

in	Applies the inbound rate to the QoS policing policy attached to applicable subscribers sessions or 802.1q VLANs.
out	Applies the outbound rate to the outbound QoS policies attached to applicable subscribers sessions or 802.1q VLANs (QoS metering, queuing, or both policies).
metering	Specifies that the rate adjustment in the outbound direction is applied only to the QoS metering policies attached to the applicable circuit.
queuing	Specifies that the rate adjustment in the outbound direction is applied only to the QoS PWFQ policies attached to the applicable circuit. PWFQ is the only type of QoS queuing policy that currently supports learned rate adjustments.
ancp	Optional. Ignores any rate update information received through TR-101 and only apply rate updates learned through ANCP.

1.49.4 Default

The system does not use the learned rates to override the rates specified by the attached QoS policies.

1.49.5 Usage Guidelines

In the subscriber configuration mode, use the **access-line rate** command to override the rates specified by the QoS policies attached to the applicable subscriber session(s) with the rates learned from the neighbor peer (DSLAM) through ANCP or TR-101 PPPoE, PPPoA, or DHCP tags.

Note: The QoS policy itself is not modified, only the terms of its enforcement on the particular circuit(s) to which the learned rates are applied.

Note: The SmartEdge router learns the rate to be applied from the Actual-Data-Rate-Downstream in the General Switch Management Protocol (GSMP) port-up message or from the Point-to-Point Protocol over Ethernet (PPPoE) or Dynamic Host Configuration Protocol (DHCP) option according to TR-101. If the **ancp** keyword is specified with the **access-line rate** command, the SmartEdge router learns the rate from ANCP. Otherwise, the SmartEdge router may also learn the rate from the Point-to-Point Protocol over Ethernet (PPPoE) or Dynamic Host Configuration Protocol (DHCP) option.

In the subscriber and dot1q profile configuration modes, use the **access-line rate out metering** command to specify that the learned outbound line rate should only be used to override the rate of any QoS metering policy attached to the applicable circuit. In the subscriber and dot1q profile configuration modes, use the **access-line rate out queuing** command to specify that the learned outbound line rate should only be used to override the rate of any QoS PWFQ policy attached to the applicable circuit. If **access-line rate out** is specified without either the **metering** or **queuing** keyword, then the outbound rate adjustments are applied to both QoS metering and PWFQ policies of the applicable circuit.

When the same QoS rate of a circuit is subject to modification from both ANCP and a RADIUS VSA such as 196, 156, or 157, the lower of the last ANCP rate received and the relevant VSA rate are applied to the circuit.

Note: More than one instance of the **access-line rate** command may be specified in a single subscriber or dot1q profile configuration record. However, only one instance of **access-line rate out** may be specified (with or without the parameters).

Note: When you configure the number of subscriber sessions to be limited to one session for each VLAN through the use of the **bind auth maximum** command (where max = 1), the SmartEdge router merges the two circuits so that the subscriber session and the parent VLAN share the same circuit. In this scenario, when a QoS PWFQ policy is applied on the circuit and a metering policy is applied under the subscriber configuration, by default outbound line rate adjustments are applied to both the metering rate on the subscriber session and the PWFQ rate configured on the VLAN. By using either the **access-line rate out queuing** or **access-line rate out metering** command, you can selectively update a PWFQ policy binding applied on the VLAN configuration or a metering policy binding provided through the RADIUS attributes of a subscriber.

In dot1q profile configuration mode, use the **access-line rate** command to override the rates specified by the QoS policies attached to a 802.1q VLAN circuit that is subject to the dot1q profile. This command overrides the rates specified by any applicable QoS policies with the learned rates from the neighbor peer (DSLAM).

If the parent circuit of the subscriber circuit has a QoS policy, then the learned rate can be applied to the QoS policy attached to the parent circuit by specifying the **access-line adjust cvlan** command. Otherwise, the learned rate is applied to the circuit with the associated circuit agent ID.

Use the **no** form of this command to disable use of learned rates to override the rates specified by the attached QoS policies.

1.49.6 Examples

The following example shows how to enable the system to use learned outbound rates to override any metering and PWFQ rates in the `out` direction for the `isp1` subscriber profile in the `access7` context, but only if the rate is learned from ANCP:

```
[local]Redback(config)#context access7
[local]Redback(config-ctx)#subscriber profile isp1
[local]Redback(config-sub)#access-line rate out ancp
```

The following example shows how to enable the system to use learned inbound rates to override any policing rate and learned outbound rates to override any metering and PWFQ rates for the 802.1 PVCs subject to dot1q profile named `adjust_all`:

```
[local]Redback(config-ctx)#dot1q profile adjust_all
[local]Redback(config-dot1q-profile)#access-line rate in
[local]Redback(config-dot1q-profile)#access-line rate out
```

The following example shows how to enable the system to use learned outbound rates to override the rates of any QoS PWFQ policies for the 802.1 PVCs subject to dot1q profile named `adjust_pwfq`:

```
[local]Redback(config-ctx)#dot1q profile adjust_pwfq
[local]Redback(config-dot1q-profile)#access-line rate out queuing
```

1.50 accounting

accounting {**in** | **out**} ***pol-type*** {***variable-name*** | **"*class-name-1* [*class-name-2*]..."**}

no accounting {**in** | **out**} ***pol-type*** {***variable-name*** | **"*class-name-1* [*class-name-2*]..."**}

1.50.1 Purpose

Enables accounting for the specified policy and class.

1.50.2 Command Mode

Service profile configuration

1.50.3 Syntax Description

in	Enables accounting for traffic received by the SmartEdge router.
out	Enables accounting for traffic transmitted by the SmartEdge router.
pol-type	Type of policy for which accounting is enabled, according to one of the following keywords: • **fwd**—Forward policy • **qos**—Quality of service (QoS) policy • **circuit**—Circuit policy

class-name-n	Class name that you have specified in the policy. You can specify up to eight class names, separated by spaces. Double quotation marks (“ ”) must surround the string of one to eight class names.
variable-name	Specifies the variable name using the **parameter value** command that contains a reference to a dynamic class or classes that are specified in the profile. The $ symbol must be the first character of the variable name.

1.50.4 Default

Accounting is disabled for all policies and classes.

1.50.5 Usage Guidelines

Use the **accounting** command to enable accounting for the specified policy and class.

Note: Forward policies do not support accounting for transmitted traffic.

Use the **no** form of this command to disable accounting for the specified policy and class.

1.50.6 Examples

The following example shows how to enable accounting for incoming traffic in the `redirect` class:

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

The following example enables accounting for incoming traffic in the `dynamic_service` profile. The `$class_bearer`variable, which is configured using the **parameter** command, contains references to the dynamic classes. In the following example, `D1` and `D2` are the names of the predefined classes:

```
[local]Redback(config-ctx)#radius service profile dynamic_service
[local]Redback(config-ctx)#parameter value %dynamic_class_qos_in “D1 D2”
[local]Redback(config-ctx)#parameter value %dynamic_class_qos_in
[local]Redback(config-svc-profile)#accounting qos in $class_bearer
```

1.51 active-timeout

active-timeout ***timeout-value***

no active-timeout*timeout-value*

1.51.1 Purpose

Configures the active timeout setting for flows that use the specified profile, in seconds.

1.51.2 Command Mode

Flow IP profile configuration

1.51.3 Syntax Description

timeout-value	Configures the active timeout setting for ling-lived flows, in seconds. If the idle timeout period has not already passed, then a flow is considered complete (expired) when the active timeout period passes, and a flow record is created and exported to the Layer 2 cache. Range is from 15 to 1800 seconds.

1.51.4 Default

The default timeout value is 1800 seconds (30 minutes).

1.51.5 Usage Guidelines

Use the **active-timeout** command to configure the active timeout setting for flows that use this profile, in seconds.

A flow expires when either of the following occurs:

- The idle timeout period passed
- The active timeout period passes

When a flow expires, a flow record is created and exported to the Layer 2 cache.

Use the **no** form of this command to return the active timeout value to the default setting of 1800 seconds.

1.51.6 Examples

The following example shows how to configure the active timeout to `1000` seconds for flows that use the profile `c1`:

```
[local]Redback#configure
[local]Redback(config)#flow ip profile c1
[local]Redback(config-flow-ip-profile)#active-timeout 1000
```

1.52 address

address {*ip-addr netmask* | *ip-addr/prefix-length* | *start-ip-addr* **to** *end-ip-addr* **port-block** *start-port-block* [**to** *end-port-block*] | *ip-addr*/**32 port-block** *start-port-block* [**to** *end-port-block*]}

no address {*ip-addr netmask* | *ip-addr/prefix-length* | *start-ip-addr* **to** *end-ip-addr*}

1.52.1 Purpose

Assigns an IP address, a range of IP addresses, or an IP address with one or more blocks of Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports to the Network Address Translation (NAT) pool.

1.52.2 Command Mode

NAT pool configuration

1.52.3 Syntax Description

ip-addr netmask	IP address and subnet mask.
ip-addr/prefix-length	IP address and prefix length.
start-ip-addr **to** *end-ip-addr*	Starting IP address to ending IP address.
ip-addr/**32**	IP address and prefix length when specifying one or more blocks of TCP/UDP port numbers.
port-block *start-port-block*	Starting port block number. The range of values is 0 to 15. Block 0 includes port 0 to port 4095.
to *end-port-block*	Optional. Ending port-block number. If not entered, assigns only the TCP/UDP port numbers in the port block specified by the *start-port-block* argument. The range of values is 1 to 15.

1.52.4 Default

All TCP/UDP port numbers for the IP address are assigned to the NAT pool.

1.52.5 Usage Guidelines

Use the **address** command to assign the IP address and subnet mask, a range of IP addresses or an IP address with a range of TCP/UDP ports that will be included in the NAT pool.

To specify port blocks, you must have an enhanced NAT license.

The TCP/UDP port number space is divided into 16 blocks. Each block contains 4,096 sequential numbers. Blocks are numbered from 0 to 15. If you specify one or more blocks of TCP/UDP ports, you must specify a prefix length of `32` or a range of IP addresses.

You can enter this command multiple times to assign multiple IP addresses, ranges of IP addresses, and an IP address with TCP/UDP port blocks to a NAT pool.

After entering the command, you can use the **exclude** command to exclude well-known ports or ranges of ports from the NAT pool (enhanced NAT feature).

Use the **no** form of this command to remove IP addresses from the NAT pool. If you enter the **no** form with an IP address that was configured with the **port-block** keyword, the IP address and all its configured port blocks are removed from the NAT pool.

1.52.6 Examples

The following example shows how to configure the NAT pool, `NAT-1`, and fill the pool with the IP address, `171.71.71.1`, with all its TCP/UDP ports and the IP address, `171.71.72.2`, with port blocks `1` to `3`:

```
[local]Redback(config)#context ISP
[local]Redback(config-ctx)#ip nat pool NAT-1 napt
[local]Redback(config-nat-pool)#address 171.71.71.1/32
[local]Redback(config-nat-pool)#address 171.71.72.2/32 port-block 0 to 3
[local]Redback(config-nat-pool)#exclude well-known
```

1.53 address-family (IS-IS)

address-family {ipv4 {unicast | multicast} | ipv6 unicast }

no address-family {ipv4 {unicast | multicast} | ipv6 unicast}

1.53.1 Purpose

Configures multitopology Intermediate System-to-Intermediate System (IS-IS) routing.

When entered in IS-IS router configuration mode, enables an address family for the IS-IS instance and enters IS-IS address family configuration mode.

When entered in IS-IS interface configuration mode, enables an address family for the IS-IS interface and enters IS-IS interface address family configuration mode.

1.53.2 Command Mode

- IS-IS interface configuration
- IS-IS router configuration

1.53.3 Syntax Description

ipv4	Specifies the IP Version 4 (IPv4) address family.
unicast	Specifies the unicast subfamily to enable unicast topology. Disables the unicast topology when used in the **no** form of this command.
multicast	Specifies the multicast subfamily to enable multicast topology. Disables the multicast topology when used in the **no** form of this command. Not available with the **ipv6** keyword.
ipv6	Specifies the IP Version 6 (IPv6) address family.

1.53.4 Default

When an IS-IS instance is created, the IPv4 unicast address family is enabled on the IS-IS instance. IPv4 multicast and IPv6 address families are disabled.

When IS-IS is enabled on an interface, the IPv4 unicast address family is enabled on the interface. IPv4 multicast and IPv6 address families are disabled.

1.53.5 Usage Guidelines

Use the **address-family** command to configure multitopology IS-IS routing. Enter this command in IS-IS interface configuration mode to enable an address family on an interface; enter it in IS-IS router configuration mode to enable an address family on an instance. Before an interface can participate in the routing for an address family, that address family must be enabled for both the instance and interface.

The multitopology IS-IS feature can generate multiple address families (topologies) for IS-IS; for example, it can enable one for an IPv4 unicast network, one for an IPv4 multicast network, and one for an IPv6 unicast network. Enter this command multiple times on a single interface or instance to create different topologies.

Multitopology IS-IS routing is useful when multiple address families are needed; for example, the reverse path forwarding (RPF) checks used by the IPv4

multicast routing protocol can use its own Interior Gateway Protocol (IGP) routing table instead of using the IPv4 unicast routing table.

The SmartEdge router supports IPv6 IS-IS routing in multitopology mode only.

For more information on multitopology IS-IS, see the Internet Draft, ***M-ISIS: Multi Topology Routing in IS-IS***, draft-ietf-isis-wg-multi-topology-06.txt.

Note: If you do not want the IPv4 unicast address family enabled on an IS-IS instance (it is enabled by default), explicitly disable it using the **no address-family** command in IS-IS router configuration mode.

Use the **no** form of this command in IS-IS interface configuration mode to disable an address family on an ISIS interface.

Use the **no** form of this command in IS-IS router configuration mode to disable an address family on an IS-IS instance.

1.53.6 Examples

The following example shows how to enable the IPv4 unicast and IPv4 multicast address families in the IS-IS instance `isis1`, enable the IPv4 unicast and IPv4 multicast address families on the `fa4/1` interface, enable the IPv4 unicast address family only on the `fa4/2` interface, and enable IPv4 multicast only on the `fa4/3` interface:

```
[local]Redback(config-ctx)#router isis isis1
[local]Redback(config-isis)#address-family ipv4 unicast
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#address-family ipv4 multicast
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#address-family ipv4 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#address-family ipv4 multicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
[local]Redback(config-isis)#interface fa4/2
[local]Redback(config-isis-if)#address-family ipv4 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
[local]Redback(config-isis)#interface fa4/3
[local]Redback(config-isis-if)#no address-family ipv4 unicast
[local]Redback(config-isis-if)#address-family ipv4 multicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
```

The following example shows how to enable the IPv4 unicast and IPv6 unicast address families in the isis2 IS-IS instance, IPv4 unicast and IPv6 unicast address families on the `fa4/1` interface, IPv4 unicast address family only on the `fa4/2` interface, and IPv6 unicast only on the `fa4/3` interface:

```
[local]Redback(config-ctx)#router isis isis2
[local]Redback(config-isis)#address-family ipv4 unicast
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#address-family ipv6 unicast
[local]Redback(config-isis-af)#exit
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#address-family ipv4 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#address-family ipv6 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
[local]Redback(config-isis)#interface fa4/2
[local]Redback(config-isis-if)#address-family ipv4 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
[local]Redback(config-isis)#interface fa4/3
[local]Redback(config-isis-if)#no address-family ipv4 unicast
[local]Redback(config-isis-if)#address-family ipv6 unicast
[local]Redback(config-isis-if-af)#exit
[local]Redback(config-isis-if)#exit
```

1.54 address-family ipv4 (BGP)

address-family ipv4{**multicast** | **unicast**}

no address-family ipv4{**multicast** | **unicast**}

1.54.1 Purpose

When entered in BGP router configuration mode, specifies the use of standard IP Version 4 (IPv4) multicast or unicast address prefixes for the Border Gateway Protocol (BGP) routing instance and enters BGP address family configuration mode.

When entered in BGP neighbor configuration mode, this command specifies the use of IPv4 multicast or unicast address prefixes for the specified BGP neighbor, and enters BGP neighbor address family configuration mode.

When entered in BGP peer group configuration mode, this command specifies the use of IPv4 multicast or unicast address prefixes for the specified BGP peer group, and enters BGP peer group address family configuration mode.

1.54.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration
- BGP router configuration

1.54.3 Syntax Description

multicast	Specifies multicast address prefixes.
unicast	Specifies unicast address prefixes.

1.54.4 Default

When entered in BGP router configuration mode, this command has no default setting.

When entered in BGP neighbor configuration mode or BGP peer group configuration mode, address prefixes are set to IPv4 multicast.

1.54.5 Usage Guidelines

Use the **address-family ipv4** command in BGP router configuration mode to specify the use of standard IPv4 unicast or multicast address prefixes for the BGP routing instance, and to enter BGP address family configuration mode. The **aggregate-address**, **dampening**, **flap-statistics**, **network**, and **redistribute** commands are available in BGP address family configuration mode. Routes are sent to BGP neighbors that have corresponding address family attributes.

Use the **address-family ipv4** command in BGP neighbor configuration mode to specify the use of IPv4 unicast or multicast address prefixes for the BGP neighbor, and to enter BGP neighbor address family configuration mode. The commands that configure the routing policies used with neighbors, **as-path-list, default-originate**, **prefix-list**, **maximum prefix, remove-private-as**, **route-map**, and **route-reflector-client**, are available in BGP neighbor address family configuration mode. To be established a BGP session, you must configure a neighbor with corresponding address family attributes.

Use the **address-family ipv4** command in BGP peer group configuration mode to specify the use of IPv4 multicast or unicast address prefixes, and to enter BGP peer group address family configuration mode. The commands that configure routing policies used with members of a peer group, **as-path-list, default-originate**, **prefix-list**, **maximum prefix, remove-private-as,** and **route-map**, are available in BGP peer group address family configuration mode.

Used in *Configuring BGP*.

Use the **no** form of this command to remove BGP address family attributes for the specified BGP instance or neighbor.

1.54.6 Examples

The following example illustrates the BGP routing process running in autonomous system `100`. In this example, the network `20.0.0.0/8` advertises BGP routing updates which are sent in unicast mode, while Open Shortest Path First (OSPF) routes are redistributed into the BGP routing domain as multicast routes. The SmartEdge router is a unicast BGP peer with the neighbor at IP address `102.210.210.1` and is a multicast peer with the neighbor at IP address `68.68.68.68`. Inbound prefix list `perf1` and outbound route map `map2` are applied in unicast mode to the neighbor at IP address `102.210.210.1`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#network 20.0.0.0/8
[local]Redback(config-bgp-af)#exit
[local]Redback(config-bgp)#address-family ipv4 multicast
[local]Redback(config-bgp-af)#redistribute ospf 100
[local]Redback(config-bgp-af)#exit
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#prefix-list pref1 in
[local]Redback(config-bgp-peer-af)#route-map map2 out
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 68.68.68.68 external
[local]Redback(config-bgp-neighbor)#remote-as 300
[local]Redback(config-bgp-neighbor)#address-family ipv4 multicast
```

1.55 address-family ipv4 mdt

`address-family ipv4 mdt`

1.55.1 Purpose

When entered in BGP router configuration mode, enables multicast distribution tree (MDT) addresses for a Border Gateway Protocol (BGP) routing instance and enters BGP address family configuration mode.

When entered in BGP router VPN configuration mode, enables MDT addresses for a BGP routing instance within a Virtual Private Network (VPN) context and enters BGP VPN address family configuration mode.

When entered in BGP neighbor configuration mode, enables MDT addresses for a specified BGP neighbor and enters BGP neighbor address family configuration mode.

1.55.2 Command Mode

- BGP neighbor configuration
- BGP router configuration

- BGP VPN router configuration

1.55.3 Syntax Description

This command has no keywords or arguments.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **address-family ipv4 mdt** command in BGP configuration mode to specify the use of MDT addresses for a BGP routing instance, and to enter BGP address family configuration mode.

Use the **address-family ipv4 mdt** command in BGP VPN configuration mode to specify the use of MDT addresses for a BGP routing instance, and to enter BGP VPN address family configuration mode.

Use the **address-family ipv4 mdt** command in BGP neighbor configuration mode to specify the use of MDT addresses for a BGP neighbor.

Note: MDT address configuration is supported for BGP in the local context and VPN contexts only. MDT address configuration is supported for BGP neighbors in the local context only. MDT address configuration is not supported for external BGP (eBGP) peers.

1.55.6 Examples

The following example shows how to enable the MDT address family for a BGP routing instance and the BGP neighbor **102.210.210.1**:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 1
[local]Redback(config-bgp)#address-family ipv4 mdt
[local]Redback(config-bgp)#neighbor 102.210.210.1 internal
[local]Redback(config-bgp-neighbor)#address-family ipv4 mdt
```

1.56 address-family ipv4 vpn

address-family ipv4 vpn

1.56.1 Purpose

When entered in BGP router configuration mode, enables Virtual Private Network (VPN)-IP Version 4 (IPv4) prefixes for a Border Gateway Protocol (BGP) routing instance and enters BGP address family configuration mode.

When entered in BGP neighbor configuration mode, enables VPN-IPv4 prefixes for a specified BGP neighbor and enters BGP neighbor address family configuration mode.

When entered in BGP peer group configuration mode, enables VPN-IPv4 prefixes for a specified BGP peer group and enters BGP peer group address family configuration mode.

1.56.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration
- BGP router configuration

1.56.3 Syntax Description

This command has no keywords or arguments.

1.56.4 Default

None

1.56.5 Usage Guidelines

Use the **`address-family ipv4 vpn`** command in BGP configuration mode to specify the use of VPN-IPv4 prefixes for a BGP routing instance, and to enter BGP address family configuration mode.

Use the **`address-family ipv4 vpn`** command in BGP neighbor configuration mode to specify the use of VPN-IPv4 prefixes for a BGP neighbor in an internal BGP (iBGP) session, and to enter BGP neighbor address family configuration mode.

Use the **`address-family ipv4 vpn`** command in BGP peer group configuration mode to specify the use of VPN-IPv4 prefixes for a specified BGP peer group, and to enter BGP peer group address family configuration mode.

Note: The **`address-family ipv4 vpn`** command cannot be used in non-local contexts.

1.56.6 Examples

The following example shows how to specify the use of route flap statistics collection for VPN-IPv4 prefixes, and enable the address family for the BGP neighbor, `102.210.210.1`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#address-family ipv4 vpn
[local]Redback(config-bgp-af)#flap-statistics
[local]Redback(config-bgp-af)#exit
[local]Redback(config-bgp)#neighbor 102.210.210.1 internal
[local]Redback(config-bgp-neighbor)#address-family ipv4 vpn
```

1.57 address-family ipv6 unicast

address-family ipv6 unicast

no address-family ipv6 unicast

1.57.1 Purpose

When entered in BGP router configuration mode, specifies the use of IP Version 6 (IPv6) unicast address prefixes for the Border Gateway Protocol (BGP) routing instance and enters BGP address family configuration mode.

When entered in BGP neighbor configuration mode, specifies the use of IPv6 unicast address prefixes for the specified BGP neighbor, and enters BGP neighbor address family configuration mode.

When entered in BGP peer group configuration mode, specifies the use of IPv6 unicast address prefixes for the specified BGP peer group, and enters BGP peer group address family configuration mode.

1.57.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration
- BGP router configuration

1.57.3 Syntax Description

This command has no keywords or arguments.

1.57.4 Default

When entered in BGP router configuration mode, this command has no default setting.

When entered in BGP neighbor configuration mode or BGP peer group configuration mode, address prefixes are set to IPv6 unicast.

1.57.5 Usage Guidelines

Use the **address-family ipv6 unicast** command in BGP router configuration mode to specify the use of standard IPv6 unicast address prefixes for the BGP routing instance, and to enter BGP address family configuration mode. Routes are sent to BGP neighbors that have corresponding address family attributes.

Use the **address-family ipv6 unicast** command in BGP neighbor configuration mode to specify the use of IPv6 unicast address prefixes for the BGP neighbor, and to enter BGP neighbor address family configuration mode. To established a BGP session, you must configure a neighbor with corresponding address family attributes.

Use the **address-family ipv6 unicast** command in BGP peer group configuration mode to specify the use of IPv6 unicast address prefixes, and to enter BGP peer group address family configuration mode.

Use the **no** form of this command to remove BGP address family attributes for the specified BGP instance or neighbor.

1.57.6 Examples

The following example illustrates the BGP routing process running in autonomous system `100`. In this example, the network, `AF26:3344:ADF7:77B5::2000/128`, advertises BGP routing updates that are sent in IPv6 unicast mode:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#router bgp 100

[local]PE1(config-bgp)#neighbor 10.10.10.2 internal

[local]PE1(config-bgp-neighbor)#address-family ipv6
unicast

[local]PE1(config-bgp-neighbor)#end
```

1.58 address-family ipv6 vpn

address-family ipv6 vpn

no address-family ipv6 vpn

1.58.1 Purpose

Enables the transport of labeled IPv6 VPN routes over an IPv4 network on a BGP neighbor.

1.58.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration
- BGP router configuration

1.58.3 Syntax Description

This command has no keywords or arguments.

1.58.4 Default

The IPv6 VPN address-family is disabled for BGP routes.

1.58.5 Usage Guidelines

Use the **address-family ipv6 vpn** command to enable the transport of labeled IPv6 VPN routes over an IPv4 network on a BGP neighbor.

Note: The **address-family ipv6 vpn** command can be configured in the local context only. Only unicast address families can be configured in the VPN context.

Use the **no** form of this command to disable the transport of labeled IPv6 VPN routes over an IPv4 network on a BGP neighbor.

1.58.6 Examples

The following example shows how to enable the transport of labeled IPv6 VPN routes over an IPv4 network on an internal neighbor with IP address 10.10.10.2. First, the transport of IPv6 routes over the MPLS IPv4 network is enabled:

```
[local]PE1(config)#context local
```

```
[local]PE1(config-ctx)#router bgp 100

[local]PE1(config-bgp)#address-family ipv6 vpn

[local]PE1(config-bgp)#end
```

Next, the IPv6 VPN address family is globally enabled for BGP:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#router bgp 100

[local]PE1(config-bgp)#neighbor 10.10.10.2 internal

[local]PE1(config-bgp-neighbor)#address-family ipv6 vpn

[local]PE1(config-bgp-neighbor)#end
```

1.59 admin-access-group

admin-access-group “*acl-name1 acl-name2 acl-name3...*” **in** [**count**] [**log**]

no admin-access-group {**“ ”** | “*acl-name1 acl-name2 acl-name3...*”}**in** [**count**] [**log**]

1.59.1 Purpose

Applies access control to all inbound packets delivered to the kernel, regardless of the interface through which packets are received.

1.59.2 Command Mode

Context configuration

1.59.3 Syntax Description

acl-name	Name of the IP ACL being applied. You can configure up to ten ACL names in one administrative access group list. You must enclose multiple ACL names in quotation marks and separate ACL names with one or more spaces. Each IP ACL name can be up to 39 alphanumeric characters long. However, ensure that the total number of characters for all ACL names referenced in the access group does not exceed 255. If you want to use ten ACLs, create names that are 24 or fewer characters long. A colon (:) is not allowed in ACL names.
in	Specifies that the IP ACL is to be applied to incoming packets.
count	Optional. Enables ACL packet counting.
log	Optional. Enables ACL packet logging.

1.59.4 Default

No administrative access control is applied.

1.59.5 Usage Guidelines

Use the **admin-access-group** command to apply access control to all inbound packets delivered to the kernel, regardless of the interface through which packets are received. This is referred to as administrative access control and is used with IP ACLs only.

If you configure multiple ACLs in an IP access group, the SmartEdge router applies the ACLs in the order they appear within the access group to produce a specific filtering behavior. The SmartEdge router appends an implicit ***deny ip any any*** rule after all configured rules are applied.

Caution!

Risk of security breach. Administrative access control is context-specific. To ensure that all inbound packets are filtered before being delivered to the kernel, you must apply an administrative ACL to each context that is configured.

When you use the **count** keyword, the system keeps track of the number of packet matches that occur. When you use the **log** keyword, the system keeps

track of the number of packets that were denied as a result of the ACL. Count and log information is displayed in the output of the **show access-group** command.

Caution!

Risk of system performance impact. By default, counting and logging of packets is disabled because these functions have an impact on system performance. To reduce the risk, we recommend that you only enable logging or counting when required for diagnostic purposes.

Use the **no** form of this command to remove the application of an ACL to traffic inbound to the kernel. Enter empty quotations marks (“ ”) to remove all associated ACL names. If you want to delete one or more (but not all) ACLs, enter their names in quotation marks.

1.59.6 Examples

The following example shows how to apply the `test_2 and filter_3` ACLs to inbound traffic for the `local` context:

```
[local]Redback(config-ctx)#admin-access-group “test_2
filter_3” in count log
```

The following example shows how to remove all ACLs from the administrative access group for the local context:

```
[local]Redback(config-ctx)#no admin-access-group “ ” in count log
```

The following example shows how to remove the ACL `ktraffic` from the administrative access group for the local context:

```
[local]Redback(config-ctx)#no admin-access-group “ktraffic” in
```

1.60 admin-group

To specify inclusion and exclusion criteria for traffic engineering (TE) link administrative groups, use the following syntax in Resource Reservation Protocol (RSVP) constraint configuration mode:

admin-group {**exclude** | **include-any** | **include-all**} ***attribute-name***

no admin-group

To specify an interface on which administrative groups are valid on your label-switched path (LSP), use the following syntax in RSVP interface configuration mode:

admin-group ***attribute-name***

no admin-group

1.60.1 Purpose

In RSVP constraint configuration mode, specifies inclusion and exclusion criteria for TE link administrative groups during Constraint Shortest Path First (CSPF) calculation. In RSVP interface configuration mode, specifies an interface on which administrative groups are valid on the LSP.

1.60.2 Command Mode

- RSVP constraint configuration
- RSVP interface configuration

1.60.3 Syntax Description

exclude	Defines an administrative group to be excluded from the LSP.
include-any	Defines an administrative group to be included in the LSP if it contains any of the attributes in the set.
include-all	Defines an administrative group to be included in the LSP if it contains all of the attributes in the set.
attribute-name	Administrative group that is defined typically by a color.

1.60.4 Default

No administrative group attribute is associated with a constraint or an interface.

1.60.5 Usage Guidelines

In RSVP constraint configuration mode, use the **admin group** command to specify inclusion and exclusion criteria for TE link administrative groups. Any link that is present in the exclude and include lists is excluded from the include list before the Shortest Path First (SPF) calculation is applied. For example, if you specify link `10.1.1.1` in an exclude and include list, the CSPF algorithm excludes the link `10.1.1.1` before the SPF calculation is applied.

In RSVP interface configuration mode, use the **admin group** command to specify an interface on which administrative groups are valid on the LSP. You

first specify link attributes using the **attribute** command (in link-attribute configuration mode) before you configure your administrative group.

With CSPF, you configure administrative groups that are associated with an LSP. You typically use link colors as values when configuring administrative groups. Each value is associated with a specific class that you define. You can define up to 32 link attributes: 32 values (0 to 31). The path names and their corresponding values must be the same on all routers within a single Multiprotocol Label Switching (MPLS) TE domain.

Use the **no** form of this command to remove the administrative group from a constraint or an interface.

1.60.6 Examples

The following example shows how to specify that the administrative group `red` be included in the LSP in RSVP constraint configuration mode:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#constraint constraint1
[local]Redback(config-rsvp-constr)#admin-group include red
```

The following example shows how to specify which administrative groups are valid on the LSP:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#interface interface1
[local]Redback(config-rsvp-if)#admin-group red
```

1.61 administrator

administrator ***admin-name*** [{**encrypted 1** ***password***} | {**password** ***password***}]

no administrator ***admin-name***

1.61.1 Purpose

Creates an administrator logon account, or selects an existing one for modification, and enters administrator configuration mode.

1.61.2 Command Mode

Context configuration

1.61.3 Syntax Description

admin-name	Alphanumeric string representing a new or existing administrator.
encrypted 1 ***password***	Optional. Alphanumeric string representing an encrypted type 1 password for the administrator account. Required only when configuring a new administrator account.
password ***password***	Optional. Alphanumeric string representing an unencrypted password for the administrator account. Required only when configuring a new administrator account.

1.61.4 Default

No administrator accounts are defined.

1.61.5 Usage Guidelines

Use the **administrator** command to create an administrator logon account, or select an existing one for modification, and enter administrator configuration mode. When creating a new administrator account, you must specify a password using either the **encrypted 1** ***password*** or **password** ***password*** construct. When specifying an existing administrator account, a password is not required.

This command also secures the console port and enables remote access to the system. Administrators can log on directly to the console, or through a Telnet or Secure Shell (SSH) session.

You can enter an unencrypted password with embedded spaces by enclosing the entire password in double quotation marks; for example, `"This is a Password with Spaces"`.

When the system generates the configuration, all administrator passwords are encrypted. Passwords are never displayed in readable text.

Use the **no** form of this command to remove the specified administrator account.

1.61.6 Examples

The following example shows how to configure an administrator with an administrator name of `admin1` and a password of `supersecret`:

```
[local]Redback(config-ctx)#administrator admin1 password supersecret
[local]Redback(config-administrator)#
```

1.62 admission-control

admission-control {**icmp** | **tcp** | **udp**}

no admission-control {**icmp** | **tcp** | **udp**}

1.62.1 Purpose

Enables or disables session limit control for the specified protocol.

1.62.2 Command Mode

- NAT policy configuration
- Policy group class configuration

1.62.3 Syntax Description

icmp	Specifies the Internet Control Message Protocol (ICMP) as the protocol for which session limit control is to be enabled.
tcp	Specifies the Transmission Control Protocol (TCP) as the protocol for which session limit control is to be enabled.
udp	Specifies the User Datagram Protocol (UDP) as the protocol for which session limit control is to be enabled.

1.62.4 Default

Session limit control is disabled for this access control list (ACL) class.

1.62.5 Usage Guidelines

Use the **admission-control** command to enable session limit control for the specified protocol. Session limit control applies only to this ACL class in this Network Address Translation (NAT) policy. You can use this command only when the action in the class is either ignore or pool, and the pool is a Network Access Port Translation (NAPT) pool.

Use the **no** form of this command to disable session limit control.

1.62.6 Examples

The following example shows how to enable TCP session limit control for the default ACL class in this NAT policy:

```
[local]Redback(config-policy-nat)#connections tcp 100
[local]Redback(config-policy-nat)#admission-control tcp
```

The following example shows how to enable TCP session limit control for `CLASS3` in this NAT policy:

```
[local]Redback(config-policy-nat)#connections tcp 100
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-group)#class CLASS3
[local]Redback(config-policy-group-class)#ignore
[local]Redback(config-policy-group-class)#admission-control tcp
```

1.63 advertise

advertise ***ip-addr*** [**interval** ***seconds***] [**node-group** ***group-name***] [**port** ***node-discovery-port-num***]

no advertise ***ip-addr***

1.63.1 Purpose

Enables the SmartEdge router to send advertisement packets to the NetOp™ Element Management System (EMS) server.

1.63.2 Command Mode

NetOp configuration

1.63.3 Syntax Description

ip-addr	IP address of the NetOp EMS server.
interval ***seconds***	Optional. Interval, in seconds, between sending advertising packets. The range of values is 10 to 86,400 (24 hours); the default value is 60.

node-group *group-name*	Optional. Text string identifying the group to which the SmartEdge router is to be assigned. If not specified, no group assignment is made.
port *node-discovery-port-num*	Optional. Port number on the NetOp EMS server that is used to listen for node advertisement packets. The range is 1 to 65, 535; the default value is 6,580.

1.63.4 Default

No advertisement packets are sent by the SmartEdge router.

1.63.5 Usage Guidelines

Use the **advertise** command to enable the sending of advertisement packets to the NetOp EMS server from the SmartEdge router. The receipt of an advertise packet allows the NetOp EMS server to auto-discover the SmartEdge router.

The SmartEdge router sends advertise packets at the specified interval. When the NetOp EMS server receives an advertise packet, the NetOp EMS server connects to the SmartEdge router, which then stops sending advertise packets. If the SmartEdge router loses communication with the NetOp EMS server, the SmartEdge router starts sending advertise packets again, unless the administrator enters the **no** form of this command.

By default, the hostname of each SmartEdge router is “Redback,” and this is the node name that is sent in the advertisement packet. To specify a different node name in the advertisement packet, use the **system hostname** command in global configuration mode.

Use the **node-group** *group-name* construct to specify a group to which the SmartEdge router is to be assigned. If you do not specify a group, then the SmartEdge router is added to the NetOp inventory database.

If the port is not the default, use the **port** *node-discovery-port-num* construct to specify the port on the NetOp EMS server that listens for Discovery packets. This port is not the port on the NetOp EMS server that connects to the SmartEdge router.

Note: The port used by the NetOp EMS server to connect to the SmartEdge router is not configurable.

Use the **no** form of this command to disable the sending of advertising packets.

1.63.6 Examples

The following example shows how to enable communication with the NetOp EMS server and send an advertising packet every 45 seconds:

```
[local]Redback(config)#netop
[local]Redback(config-netop)#advertise 10.1.1.1 interval 45 node-group G10 port 6080
```

1.64 advertise-interval

advertise-interval{*interval* | **millisecond** *interval*}

{**no** | **default**} **advertise-interval**

1.64.1 Purpose

Configures the interval at which Virtual Router Redundancy Protocol (VRRP) advertisements are sent out from the specified interface.

1.64.2 Command Mode

VRRP configuration

1.64.3 Syntax Description

interval	Amount of time, in seconds, between VRRP advertisements. The range of values is 1 to 254; the default value is 1.
millisecond *interval*	Amount of time, in milliseconds, between VRRP advertisements. The range of values is 100 to 999.(1)

(1) This construct is supported for IPv4 only.

1.64.4 Default

VRRP advertisements are sent out every second.

1.64.5 Usage Guidelines

Use the **advertise-interval** command to determine the frequency of VRRP advertisements sent from the specified interface. This command is useful for troubleshooting misconfigured routers.

VRRP fast advertisement (using the **millisecond** *interval* construct) is supported for IPv4 only. If millisecond granularity is configured, VRRP authentication is not supported.

Note: The **advertise-interval** command is available for PPA2 cards only.

Use the **no** or **default** form of this command to return the interval to its default value of 1.

1.64.6 Examples

The following example shows how to configure the interface, `eth0`, to send VRRP advertisements every `20` seconds:

```
[local]Redback(config)#interface eth0
[local]Redback(config-if)#vrrp 1 owner
[local]Redback(config-vrrp)#advertise-interval 20
```

1.65 advertise max-interval

advertise max-interval ***max-int***

no advertise max-interval ***max-int***

1.65.1 Purpose

Specifies the maximum interval between advertisement messages sent by the foreign-agent (FA) instance to the mobile nodes (MNs).

1.65.2 Command Mode

Mobile IP interface configuration

1.65.3 Syntax Description

max-int	Maximum interval (in seconds) between advertisement messages. The range of values is 4 to 1800 seconds; the default value is 600 seconds (10 minutes).

1.65.4 Default

The maximum interval between advertisement messages is 600 seconds.

1.65.5 Usage Guidelines

Use the **advertise max-interval** command specify the maximum interval between advertisement messages sent by the FA instance or HA instance to the mobile nodes.

Use the **no** form of this command to specify the default condition.

1.65.6 Examples

The following example shows how to specify `300` seconds as the maximum interval between advertisement messages:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mn-access
[local]Redback(config-mip-if)#advertise max-interval 300
```

1.66 advertise max-lifetime

advertise max-lifetime ***max-life***

no advertise max-lifetime ***max-life***

1.66.1 Purpose

Specifies the maximum amount of time that an advertisement message sent by the foreign-agent (FA) instance to the mobile node (MN) is valid in the absence of further advertisement messages.

1.66.2 Command Mode

Mobile IP interface configuration

1.66.3 Syntax Description

max-lifetime ***max-life***	Amount of time (in seconds) that an advertisement message is valid in the absence of further advertisement messages. The minimum value equals the value of the ***max-int*** argument set by the **advertise max-interval** command (in Mobile IP interface configuration mode); the maximum value is 9000 seconds (150 minutes). The default value is three times the value of the ***max-int*** argument set by the **advertise max-interval** command.

1.66.4 Default

The maximum advertisement lifetime is three times the value of the ***max-int*** argument set by the **advertise max-interval** command.

1.66.5 Usage Guidelines

Use the **advertise max-lifetime** command to specify the maximum amount of time that an advertisement message sent by the FA instance or HA instance to the mobile node is valid in the absence of further advertisement messages.

Use the **no** form of this command to specify the default condition.

1.66.6 Examples

The following example shows how to specify `900` seconds as the maximum lifetime of an advertisement message:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mn-access
[local]Redback(config-mip-if)#advertise max-lifetime 900
```

1.67 advertise min-interval

advertise min-interval ***min-int***

no advertise min-interval ***min-int***

1.67.1 Purpose

Specifies the minimum interval between advertisement messages sent by the foreign-agent (FA) instance to the mobile node (MN).

1.67.2 Command Mode

Mobile IP interface configuration

1.67.3 Syntax Description

min-int	Minimum interval (in seconds) between advertisement messages. The range of values is 3 to 1800 seconds; the default value is 0.75 times the value of the ***max-int*** argument for the **advertise max-interval** command (in Mobile IP interface configuration mode).

1.67.4 Default

The minimum advertisement interval is 0.75 times the value of the ***max-int*** argument for the **advertise max-interval** command.

1.67.5 Usage Guidelines

Use the **advertise min-interval** command to specify the minimum interval between advertisement messages sent by the FA instance or HA instance to the mobile node.

Use the **no** form of this command to specify the default condition.

1.67.6 Examples

The following example shows how to specify `200` seconds as the minimum interval between advertisement messages:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mn-access
[local]Redback(config-mip-if)#advertise min-interval 200
```

1.68 advertise tunnel-type

advertise tunnel-type gre

no advertise tunnel-type gre

1.68.1 Purpose

Advertises Generic Routing Encapsulation (GRE) tunnel types sent by the foreign-agent (FA) instance to mobile nodes (MNs).

1.68.2 Command Mode

FA configuration

1.68.3 Syntax Description

gre	Specifies that Generic Routing Encapsulation (GRE) tunnels are advertised to mobile nodes.

1.68.4 Default

IP-in-IP tunnels are advertised implicitly; no GRE tunnel types are advertised.

1.68.5 Usage Guidelines

Use the **advertise tunnel-type** command to advertise GRE tunnel types in the mobility agent advertisement extension in the ICMP Router Advertisement (RA) message.

Use the **no** form of this command to specify the default condition.

1.68.6 Examples

The following example shows how to advertise the GRE tunnel type:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#advertise tunnel-type gre
```

1.69 advertisement-interval

advertisement-interval *interval*

no advertisement-interval *interval*

1.69.1 Purpose

Modifies the minimum interval at which Border Gateway Protocol (BGP) routing updates are sent to the specified neighbor or members of the specified peer group.

1.69.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.69.3 Syntax Description

interval	Minimum interval, in seconds, at which BGP routing updates are sent. The range of values is 0 to 600. For external BGP (eBGP), the default value is 30. For internal BGP (iBGP), the default value is 5.

1.69.4 Default

The default advertisement interval is 30 seconds for eBGP and 5 seconds for iBGP.

1.69.5 Usage Guidelines

Use the **advertisement-interval** command to set the minimum interval at which BGP routing updates are sent to the specified neighbor or members of the specified peer group.

The Minimum Route Advertisement Interval (MRAI) starts when an UPDATE message is sent to a BGP neighbor or peer group. After sending an UPDATE message to the specified BGP peers, the router waits for the specified MRAI before sending the next UPDATE message the peers. If a route change occurs and the MRAI has passed since the last UPDATE message was sent, the router immediately sends an UPDATE message to the peer. If a route change occurs and the MRAI has not passed since the last UPDATE message was sent to the peer, the router waits for the specified MRAI before sending a new UPDATE message.

Consider an example where the MRAI is set to 20 seconds:

- The first route change occurs, so the BGP router immediately sends an UPDATE message to the specified peers and starts the MRAI. (The first route change always occurs at 0 seconds according to the MRAI).
- A second route change occurs 2 seconds after the MRAI starts. In this case the router waits 18 more seconds before sending an UPDATE message to the specified peers. The router restarts the MRAI after sending the UPDATE message to the specified peers.
- A third route change occurs at 60 seconds. Because 40 seconds passed since the last UPDATE message was sent (40 seconds is greater than the configured MRAI of 20 seconds), the router immediately sends the third UPDATE message to the specified peers.

Note: This command cannot be enabled on neighbors that belong to a peer group.

Use the **no** form of this command to restore the advertisement interval to its default value.

1.69.6 Examples

The following example shows how to send unicast routing updates every `60` seconds to the neighbor at IP address `102.210.210.1`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#advertisement-interval 60
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#
```

The following example displays output from the **show bgp neighbor** command for the configuration in the previous example:

```
[local]Redback>show bgp neighbor 10.100.1.102


BGP neighbor: 102.210.210.1, remote AS: 64001, internal link
Version: 4, router identifier: 102.210.210.1
State: Established for 00:30:10
.
.
.
Minimum time between advertisement runs: 60 secs
```

1.70 aggregate-address

aggregate-address {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**as-set**] [**component-map** *map-name*] [**attribute-map** *map-name*] [**summary-only**]

no aggregate-address {*ip-addr/prefix-length* | *ipv6-addr/prefix-length*} [**as-set**] [**component-map** *map-name*] [**attribute-map** *map-name*] [**summary-only**]

1.70.1 Purpose

Creates an aggregate entry in the Border Gateway Protocol (BGP) database for the BGP address family.

1.70.2 Command Mode

BGP address family configuration

1.70.3 Syntax Description

ip-addr/prefix-length	Specifies the IP address, in the form ***A.B.C.D***, and the prefix length, separated by the slash (**/**) character. The range of values for the ***prefix-length*** argument is 0 to 32.
ipv6-addr/prefix-length	Specifies the IP Version 6 (IPv6) address, in the form ***A:B:C:D:E:F:G:H***, and the prefix length, separated by the slash (**/**) character. The range of values for the ***prefix-length*** argument is 0 to 128.
as-set	Optional. Generates autonomous system (AS) set path information.
component-map ***map-name***	Optional. Name of the route map used to select the routes to create an aggregate entry.
attribute-map ***map-name***	Optional. Name of the route map used to set the attribute of the aggregate route.
summary-only	Optional. Suppress the advertisement of specific routes to all neighbors. When you include the **summary-only** keyword, only the aggregate address is advertised to the neighbors.

1.70.4 Default

The command is disabled.

1.70.5 Usage Guidelines

Use the **aggregate-address** command to create an aggregate entry in a unicast or multicast BGP database for the BGP address family. You can implement aggregate routing in BGP by either redistributing an aggregate route into the BGP routing domain or by using this feature.

Use this command with no arguments to create an aggregate entry in the BGP routing table when any more-specific BGP routes that fall into the specified range are available. The origin of the aggregate route is advertised as the local autonomous system.

Use the **as-set** keyword to create an aggregate entry in the BGP routing table and to advertise the origin of the aggregate route as an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the command when aggregating many paths, because this route must be continually updated as autonomous system path reachability information for the summarized routes changes.

Use the **summary-only** keyword to create an aggregate address entry (for example, 10.0.0.0/7) but suppress the advertisement of more specific routes

to all neighbors. In this case, only the aggregate address is advertised to the neighbors.

Use the **no** form of this command to remove an aggregate entry.

1.70.6 Examples

The following example shows how to create an aggregate entry in the BGP routing table as long as there are more-specific routes in the `11.0.0.0/8` address block:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 64000
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#aggregate-address 11.0.0.0/8
```

1.71 aggregation-cache-size

aggregation-cache-size ***number-of-entries***

no aggregation-cache-size ***number-of-entries***

1.71.1 Purpose

Configures the maximum aggregation cache size for flows in an RFlow profile.

1.71.2 Command Mode

Flow IP profile configuration

1.71.3 Syntax Description

number-of-entries	Maximum number of entries that can be stored in the aggregation cache at one time. This determines how much information is reported when you access the RFlow data. Range is from 1024 through 32768 entries.

1.71.4 Default

The default number of entries that can be stored in the aggregation cache at one time is 4096.

1.71.5 Usage Guidelines

Use the **aggregation-cache-size** command to configure the maximum aggregation cache size for flows in an RFlow profile.

Note: To ensure optimal RFlow performance, we recommend setting the aggregation cache size to a number that is a power of 2; for example, 1024.

Use the **no** form of this command to return the aggregation cache to a default maximum size of 4096 entries.

1.71.6 Examples

The following example shows how to configure the flow aggregation cache maximum size to `1024` entries in the RFlow profile `c1`:

```
[local]Redback#configure
[local]Redback(config)#flow ip profile p1
[local]Redback(config-flow-ip-profile)#aggregation-cache-size 1024
```

1.72 aging-time

aging-time ***aging-time***

{**no** | **default**} **aging-time**

1.72.1 Purpose

Specifies the minimum time after which inactive learned medium access control (MAC) addresses are deleted for all circuits that are bound to an interface that is associated with this bridge.

1.72.2 Command Mode

Bridge configuration

1.72.3 Syntax Description

aging-time	Configured address age time in seconds. The actual aging time can differ from the configured aging time. See the Usage Guidelines. Enter a value from 10 to 75,900; the default value is 300.

1.72.4 Default

300 seconds (5 minutes).

1.72.5 Usage Guidelines

Use the **aging-time** command to specify the minimum time after which inactive learned MAC addresses are deleted for all circuits that are bound to an interface that is associated with this bridge.

The actual aging time can differ from the configured aging time. The actual aging time depends on the value of the ***aging-time*** argument:

- If you configure a value ***n*** <= 450 seconds, the actual aging time varies between ***n*** and **2*** ***n*** seconds.
- If you configure a value ***n*** > 450 seconds, the actual aging time varies between ***n*** and (***n*** + 600) seconds -- if ***n*** is not a multiple of 300 seconds; however if ***n*** is a multiple of 300 seconds, the actual aging time varies between ***n*** and (***n*** + 300) seconds.

Use the **no** or **default** form of this command to specify the default aging time for all circuits.

1.72.6 Examples

The following example shows how to specify an aging time of `18,000` seconds (5 hours):

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#bridge isp1
[local]Redback(config-bridge)#aging-time 18000
```

1.73 alarm low-partition-space

alarm low-partition-space raise-at ***raise_percentage*** **clear-at** ***clear_percentage***

{no | default} alarm low-partition-space

1.73.1 Command Mode

SSE partition configuration

1.73.2 Syntax Description

raise-at ***raise_percentage***	Partition capacity percentage at which to trigger an alarm. Range: 50 to 100.
clear-at ***clear_percentage***	Partition capacity percentage at which to clear an alarm. The ***clear_percentage*** value must be less than or equal to the ***raise_percentage*** value. Range: 10 to 100.

1.73.3 Default

An alarm is triggered when the partition is 80% full and cleared when the partition is 70% full.

1.73.4 Usage Guidelines

Generates an alarm when partition space is low.

1.73.5 Examples

In the following example, an alarm is triggered when the partition is 70% full, and cleared when the partition capacity is reduced to 65%:

```
[local]Redback(config)#sse group sse_group_1
[local]Redback(config-SE-group)#partition p01 size 5
disk 1
[local]Redback(config-SE-partition)#alarm low-partition-space raise-at 70 clear-at 65
```

1.74 alarm-report-only

alarm-report-only ***path-alarm-types***

{**no** | **default**} **alarm-report-only** ***path-alarm-types***

1.74.1 Purpose

Enables the Packet over SONET/SDH (POS) or Asynchronous Transfer Mode Optical Carrier (ATM OC) port to remain up when the SmartEdge router receives the specified alarms.

1.74.2 Command Mode

- ATM OC configuration
- port configuration

1.74.3 Syntax Description

path-alarm-types	The type or types of alarms that are allowed without shutdown of the port. Enter any combination of the following keywords: • **ais-p**—Specifies the alarm indication signal path alarm. • **rdi-p**—Specifies the remote defect indication path alarm. • **lop-p**—Specifies the loss of pointer path alarm. • **uneq-p**—Specifies the unequipped path alarm. • **plm-p**—Specifies the payload label mismatch path alarm.

1.74.4 Default

The reception of a path alarm causes the router to shut down the port.

1.74.5 Usage Guidelines

Use this command to enable the POS or ATM OC port to remain up when the SmartEdge router receives the specified alarms.

Ignoring an alarm does not completely mask it. When you configure this command for a particular alarm, the system still logs the alarm and displays it in the **show port** command (with the **detail** keyword), but the system does not shut down the port. You can use successive calls to this command to cumulatively build a list of alarms that do not trigger a port shutdown.

Use the **no** or **default** form of this command to specify which alarm or alarms cause the SmartEdge router to shut down the port.

To view the state of alarm reporting, use the **show configuration** command (in any mode) or use the **show port detail** command (in any mode).

1.74.6 Examples

The following example shows how to enable ATM port `1/1` to remain functional even if the router receives a `PLM-P` alarm:

```
[local]Redback(config)#port atm 1/1
[local]Redback(config-atm-oc)#alarm-report-only plm-p
```

1.75 alarms

alarms

no alarms

1.75.1 Purpose

In malicious-traffic configuration mode, configures alarm parameters for malicious traffic and enters malicious-traffic alarms configuration mode. In malicious-traffic context configuration mode, enables an alarm to be generated when the counters for malicious traffic reach a certain threshold.

1.75.2 Command Mode

- malicious-traffic configuration mode
- malicious-traffic context configuration mode

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

None

1.75.5 Usage Guidelines

Use the **alarms** command in malicious-traffic configuration mode to configure alarm parameters for malicious traffic and access malicious-traffic alarms configuration mode. In malicious-traffic context configuration mode, use this command to enable an alarm to be generated when the counters for malicious traffic reach a certain threshold. Before configuring this parameter in malicious-traffic context configuration mode, you must first configure counters by using the **counters** command.

Use the **no** form of this command to disable or remove the alarm. In the context configuration mode, the **no** form of this command disables the alarm for the context.

For information about detecting and monitoring malicious traffic, see *Configuring Malicious Traffic Detection and Monitoring*.

1.75.6 Examples

The following example shows how to enter malicious-traffic alarms configuration mode to configure alarm parameters for malicious traffic:

```
[local]Redback(config)#malicious-traffic

[local]Redback(config-malicious-traffic)#alarms

[local]Redback(config-malicious-traffic-alarms)#
```

The following example shows how to enter malicious-traffic context configuration mode to enable an alarm to be generated when the counters for malicious traffic reach a certain threshold.

```
[local]Redback(config-ctx)#malicious-traffic

[local]Redback(config-ctx-malicious-traffic)#alarms
```

1.76 algorithm

algorithm {**priority** | **load-balance** | **weighted-round-robin**}

{**default** | **no**} **algorithm**

1.76.1 Purpose

Assigns the algorithm used to distribute Point-to-Point Protocol (PPP) sessions among the peers in a Layer 2 Tunneling Protocol (L2TP) group.

1.76.2 Command Mode

L2TP group configuration

1.76.3 Syntax Description

priority	Assigns the next session to the highest priority peer that has not been labeled “dead”.
load-balance	Assigns the next session to the peer that has the fewest sessions.
weighted-round-robin	Assigns the next session based on calculated priority (weight).

1.76.4 Default

The algorithm is set to strict priority.

1.76.5 Usage Guidelines

Use the **algorithm** command to assign the algorithm used to distribute PPP sessions among the peers in an L2TP group. The three algorithm keywords represent distinctly different strategies for session distribution.

Use the **priority** keyword to assign a strict priority algorithm. Using this algorithm, sessions are directed to the peer with the highest priority until connection with that peer is no longer possible; then sessions are directed to the peer with the next highest priority. With this algorithm, you can assign a preference value to each peer using the **peer** command in L2TP group configuration mode; a peer with a preference value of 1 has the highest priority. Peers with equal preference values are assigned sessions using load balancing.

Use the **load-balance** keyword to assign a load-balancing algorithm. Using this algorithm, the next session is directed to the peer with the fewest sessions. The result is that the sessions are distributed across the peers equally. The peers may still have priorities assigned, but they are ignored.

Use the **weighted-round-robin** keyword assign a weighted-round-robin algorithm to calculate the priority. Using this algorithm, sessions are directed to the peer with the highest calculated priority until connection with that peer is no longer possible; then sessions are directed to the peer with the highest calculated priority. With this algorithm, you can assign a weight value to each peer using the **peer** command in L2TP group configuration mode; the weight value is used to calculate the priority. The peer with the lowest priority receives the most sessions.

Each algorithm is subject to the maximum number of tunnels and the maximum number of sessions (specified with the **max-tunnels** and **max-sessions** commands in L2TP peer configuration mode, respectively) configured for the peers that are members of the group. For example, if the strict priority algorithm is specified and the maximum sessions limit is reached on the highest priority peer, additional sessions are sent to the next highest priority peer.

Note: The SmartEdge router supports only Remote Authentication Dial-In User Service (RADIUS) servers that support tunnel extensions. If the RADIUS server does not supply the Tunnel-Preference attribute, the SmartEdge router chooses the preference for the peers arbitrarily. We recommend that you specify either the strict-priority distribution (which sets the priority of peers explicitly), or the weighted-round-robin algorithm.

For more information about configuring RADIUS, see the *Configuring RADIUS*.

Use the **default** or **no** form of this command to set the algorithm to strict priority.

1.76.6 Examples

The following example shows how to create an L2TP group, group1, with L2TP peer members, 1peer and 2peer.

First, the L2TP group, group1, is created. Two peer members, 1peer and 2peer, are then established as members of the group, and the group is configured to use strict-priority session distribution:

```
[local]Redback(config-ctx)#l2tp-group name group1
[local]Redback(config-l2tp-group)#algorithm priority
[local]Redback(config-l2tp-group)#peer name 1peer preference 10
[local]Redback(config-l2tp-group)#peer name 2peer preference 20
```

With strict-priority distribution, sessions with usernames of the form ***user***`@group1` are tunneled to `1peer` (because it has a lower preference value), as long as `1peer` is reachable and its maximum sessions threshold has not been exceeded. If `1peer` becomes unreachable or its maximum sessions threshold is reached, sessions are tunneled to `2peer`.

If the **load-balance** keyword was used instead of the **priority** keyword, the first session of the form ***user***`@group1` would be tunneled to `1peer`, and the next session for the same group would be tunneled to `2peer`, balancing the session count between them, unless one peer becomes unreachable or the maximum sessions threshold is reached.

1.77 alias

alias {**exec** | **inherit** | ***mode***} ***alias-name command-string***

no alias {**exec** | **inherit** | ***mode***} ***alias-name***

1.77.1 Purpose

Defines an alias for a command.

1.77.2 Command Mode

Global configuration

1.77.3 Syntax Description

exec	Specifies that the macro be available (in exec mode).
inherit	Defines the alias in all modes.
mode	Configuration mode in which the alias is available; see Table 3 for exceptions.

alias-name	Alias name.
command-string	Command string to be substituted for the alias.

1.77.4 Default

None

1.77.5 Usage Guidelines

Use the **alias** command to define an alias for a command. A command alias is a character string that you can use in place of a command string. Aliases are typically used to create shortcuts for frequently used commands. When aliases are defined, the software examines each command for a match in the alias table. If the system finds an alias match, it replaces the alias with the associated command string prior to processing the command.

Table 3 lists all mode prompt and keyword exceptions for the **alias** command. Except for those listed in Table 3, the keyword for the ***mode*** argument is the command mode prompt. For a list of all keywords, see the command-line interface (CLI) online Help.

Table 3 Exceptions for the alias Command

Mode Description	Mode Prompt	Mode Keyword
Network Address Translation (NAT) access control list	`policy-acl`	**nat-policy-acl**
NAT access control list class	`policy-acl-class`	**nat-policy-acl-class**

Caution!

Risk of disabled commands. It is possible to create an alias that disables existing commands. To reduce the risk, use care when you define aliases. Avoid defining an alias name that is a SmartEdge router command keyword or a partial keyword. Aliases apply to all users on a system.

You can bypass alias processing for a single command by beginning a command line with the backslash (\) character.

Use the **no** form of this command to remove an alias.

1.77.6 Examples

The following example shows how to define the alias, `sc`, (in exec mode) as `show configuration`:

```
[local]Redback(config)#alias exec sc show configuration
[local]Redback>sc

Building configuration...

Current configuration:
!
!  Configuration last changed by user 'test' at Wed Jan 29 11:20:03  2003
!
context local
port ethernet 7/1
!
end
```

The following example shows how the definition of an alias can cause unexpected problems. The first example defines the alias, `sh`, (in all modes) as `show configuration`:

```
[local]Redback(config)#alias inherit sh show configuration
```

As a result, **`show chassis`** command is disabled; the **`show chassis`** command is interpreted to mean **`show configuration chassis`**, which results in an error.

For more information on the **`show configuration`** command, see *Using the CLI*.

The following example demonstrates the use of the backslash character (\) to disable alias processing for the command:

```
[local]Redback>\sh chassis
```

1.78 all-ports

`all-ports password` ***`password`*** **`card`** ***`card-type`*** **`slot`** ***`slot-id`***

`no all-ports`

1.78.1 Purpose

Enables the operation of ports 5-8 of a *Channelized OC-3/STM-1 or OC-12/STM-4* line card in the specified chassis slot.

1.78.2 Command Mode

License configuration

1.78.3 Syntax Description

password ***password***	Specifies the password provided when the all-ports license is purchased.
card ***card-type***	Specifies the card type. Currently, only the *Channelized OC-3/STM-1 or OC-12/STM-4* line card is supported. Enter `ch-oc3oc12-8or2-portch-oc3oc12-8or2-port`
slot ***slot-id***	Specifies the chassis slot where you install the license and the line card.

1.78.4 Default

No active all-port software licenses.

1.78.5 Usage Guidelines

- When you apply this command, a message is logged to indicate that the software license has been applied.
- Currently, no per-chassis line card licenses are available. Only per-slot licenses are available.
- Per-slot software license information is shown in the *show licenses* CLI command.
- The **no all ports** command removes all all-port software licenses.
  - The **slot** ***slot-id*** option is not available. The licenses of all slots are removed by this command.
  - When you remove a license, a message is logged to indicate that the software license has been removed.

1.78.6 Examples

```
[local]dennys#config
Enter configuration commands, one per line, 'end' to exit
[local]dennys(config)# software license
[local]dennys(config-license)#all-ports password 78vvb ch-oc3oc12-8or2-port slot 2
```

1.79 allow

allow {**context name** *ctx-name* | **domain name** *name* | **pppoe service-name** *name* | **dhcp hostname** *name*}

no allow {**context name** *ctx-name* | **domain name** *name* | **pppoe service-name** *name* | **dhcp hostname** *name*}

1.79.1 Purpose

Allows access to the specified context, Point-to-Point over Ethernet (PPPoE) service, or domain for PPPoE subscriber sessions that are attached to the service policy. This command also allows a DHCP client host access to the circuit that is associated with the service policy.

1.79.2 Command Mode

Service policy configuration

1.79.3 Syntax Description

context name *ctx-name*	Allows subscriber sessions access to the specified context.
domain name *name*	Allows subscriber sessions access to the specified domain.
pppoe service-name *name*	Allows PPPoE Active Discovery Initiation (PADI) or PPPoE Active Discovery Request (PADR) packets access to the specified PPPoE service.
dhcp hostname *name*	Allows the specified DHCP client host access to the circuit that is associated with the service policy.

1.79.4 Default

None

1.79.5 Usage Guidelines

Use the **allow** command to allow access to the specified context, PPPoE service, or domain for subscriber PPPoE sessions that are attached to the service policy. You can also use the **allow** command to allow a DHCP client host to access the circuit that is associated with the service policy.

Any DHCP hosts, contexts, PPPoE services, or domains that are not explicitly specified by this command are implicitly denied. Note that the SmartEdge router does not support both allow and deny in the same service profile.

Use the **no** form of this command to remove access to the specified context, PPPoE service, or domain. Or, you can use the **no** form of this command to remove a configuration that allows a DHCP client host to access the circuit that is associated with the service policy.

1.79.6 Examples

The following example shows how to create a service policy called `local-only`, which allows subscribers access to the `local` context and denies access to all other contexts:

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#allow context name local
```

The following example shows how to create a service policy called `AllowVoice`, which allows the PPPoE service named `voice` and denies all other PPPoE services:

```
[local]Redback(config)#service-policy name AllowVoice
[local]Redback(config-policy-svc)#allow pppoe service-name voice
```

The following example shows how to create a service policy called allow`hosts`, which allows the DHCP client hosts named `group2, group3,` and `group7` to access the circuit that is associated with the specified service policy and denies all other DHCP client hosts access to the given circuit:

```
[local]Redback(config)#service-policy name allowhosts
[local]Redback(config-policy-svc)#allow dhcp hostname group2
[local]Redback(config-policy-svc)#allow dhcp hostname group3
[local]Redback(config-policy-svc)#allow dhcp hostname group7
```

1.80 allow-duplicate-mac

allow-duplicate-mac

no allow-duplicate-mac

1.80.1 Purpose

Allows Dynamic Host Control Protocol (DHCP) server subscribers to share the same medium access control (MAC) address.

1.80.2 Command Mode

DHCP server configuration

1.80.3 Syntax Description

This command has no keywords or arguments.

1.80.4 Default

Duplicate MAC addresses are not allowed.

1.80.5 Usage Guidelines

Use the **allow-duplicate-mac** command to allow DHCP server subscribers to share the same MAC address.

Note: Do not use the **allow-duplicate-mac** command within a context that has CLIPS subscribers.

Use the **no** form of this command to specify the default condition.

1.80.6 Examples

The following example shows how to enables DHCP clients with the same MAC address to be assigned IP addresses on different circuits for the DHCP internal server in the `dhcp` context:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#allow-duplicate-mac
```