Commands: s through show a

COMMAND DESCRIPTION

16/190 82-CRA 119 1170/1-V1 Uen J

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Command Descriptions

Commands starting with “s” through commands starting with “show a” 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 sa-filter

`sa-filter` [**`in`** | **`out`**] ***`acl-name`***

`no sa-filter` [**`in`** | **`out`**] ***`acl-name`***

1.1.1 Purpose

Specifies an access control list (ACL) to filter source active (SA) messages coming in to, or going out of, the peer.

1.1.2 Command Mode

MSDP peer configuration

1.1.3 Syntax Description

`in`	Optional. Filters incoming SA messages only.
`out`	Optional. Filters outgoing SA messages only.
`acl-name`	Name of the ACL used to filter SA messages.

1.1.4 Default

None

1.1.5 Usage Guidelines

Use the **`sa-filter`** command to specify an ACL to filter SA messages coming in to, or going out of, the peer.

Use the **`no`** form of this command to remove the SA filter.

1.1.6 Examples

The following example shows how to filter incoming SA messages from a peer using the ACL, **peer-sa-filter-in-group:**

```
[local]Redback(config-ctx)#ip access-list peer-sa-filter-in-group
[local]Redback(config-access-list)#seq 10 deny ip any 224.137.0.0 0.0.255.255
[local]Redback(config-access-list)#seq 20 deny ip any 224.134.1.0 0.0.0.255
[local]Redback(config-access-list)#seq 30 deny ip any host 224.131.1.1
[local]Redback(config-access-list)#seq 40 permit any any
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#peer 10.200.1.2 local-tcp-source lo1
[local]Redback(config-msdp-peer)#sa-filter in peer-sa-filter-in-group
```

The following example shows how to filter outgoing SA messages to a peer using the ACL, **peer-sa-filter-out-source-group:**

```
[local]Redback(config-ctx)#ip access-list peer-sa-filter-out-source-group
[local]Redback(config-access-list)#seq 10 deny ip 44.1.1.0 0.0.0.255 host 224.133.1.2
[local]Redback(config-access-list)#seq 20 deny ip 44.1.1.0 0.0.0.255 224.136.2.0 0.0.0.255
[local]Redback(config-access-list)#seq 30 permit ip any any
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#peer 10.200.1.2 local-tcp-source lo1
[local]Redback(config-msdp-peer)#sa-filter out peer-sa-filter-out-source-group
```

1.2 sample-interval

`sample-interval` ***`minutes`***

`default sample-interval`

1.2.1 Purpose

Specifies the interval between the collection of bulkstats samples.

1.2.2 Command Mode

bulkstats configuration

1.2.3 Syntax Description

minutes	Interval, in minutes, between samples. The range of values is 1 to 1,440 minutes (24 hours); the default value is 15 minutes.

1.2.4 Default

The sampling interval is 15 minutes.

1.2.5 Usage Guidelines

Use the **sample-interval** command to specify the interval between the collection of bulkstats samples. Setting the sampling interval so that sampling occurs too often can decrease the performance of the SmartEdge router.

Use the **default** form of this command to return the sampling interval to 15 minutes.

1.2.6 Examples

The following example shows how to set the sampling interval to **30** minutes:

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

[local]Redback(config-ctx)#bulkstats policy bulk

[local]Redback(config-bulkstats)#sample-interval 30
```

1.3 sampling

sampling

no sampling

1.3.1 Purpose

Use the **sampling** command to enable random sampling for flows using a specific IP profile.

1.3.2 Command Mode

Flow IP profile configuration

1.3.3 Syntax Description

This command has no keywords or arguments.

1.3.4 Default

Sampling is disabled.

1.3.5 Usage Guidelines

Use the **sampling** command to enable random sampling for flows using a specific IP profile.

Use the no version of this command to disable random sampling for flows using a specific IP profile.

1.3.6 Examples

The following example shows how to use the **sampling** command to enable random sampling for flows using the IP profile **p1**:

```
[local]Redback# configure
[local]Redback(config)# flow ip profile p1
[local]Redback(config-flow-ip-profile)#sampling
```

1.4 satop

satop

1.4.1 Purpose

Enable SAToP configuration mode on an attachment circuit.

1.4.2 Command Mode

E1 or DS1 Channel Config Mode.

1.4.3 Syntax Description

None.

1.4.4 Default

SAToP is not enabled.

1.4.5 Usage Guidelines

When in SAToP mode, an E1 or DS1 channel is implicitly applied as unframed. If the you do not intend to configure SAToP parameters but you want the CES channel to operate as SAToP, then you must explicitly configure the channel to unframed (for example, using the CLI command **framing unframed**).

1.4.6 Examples

The following example shows how to enable SAToP on an E1 attachment circuit.:

```
[local]Redback(config)#port e1 1/1:1:1
Redback(config-e1-ces)#l2vpn local
Redback(config-e1-ces)#satop
Redback(config-e1-satop)#
```

1.5 save configuration

save configuration [*url*] [**-noconfirm**]

1.5.1 Purpose

Saves the running configuration to a file on a remote server or the local file system.

1.5.2 Command Mode

Exec (10)

1.5.3 Syntax Description

url	Optional. URL of the file to which the configuration is saved; if not specified the configuration is saved to redback.cfg file.
-noconfirm	Optional. Replaces an existing file without prompting for confirmation.

1.5.4 Default

Commands are saved to the default configuration file.

1.5.5 Usage Guidelines

Use the **save configuration** command to save the running configuration to a file on a remote server or the local file system.

Only those commands that modify the default configuration of the SmartEdge router are saved.

When saving the configuration to the local file system, the URL takes the following form:

[/*device*][/*directory*]/*filename.ext*

The value for the *device* argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the *device* argument, the default value is the device in the current working directory. If you do not specify the *directory* argument, the default value is the current directory. Directories can be nested. The value for the *filename* argument can be up to 256 characters in length.

The value for the *filename* argument can be up to 256 characters in length. If you do not specify the *filename.ext* argument, the configuration is saved to the *redback.cfg* file.

To ensure that the binary database file (/flash/redback.bin) is created correctly when saving to the *redback.cfg* file, enter this command without a filename, or specify redback.cfg as the filename without a device or directory. For information about these files, see *Managing Configuration Files*.

When saving the configuration to a remote server, you can use the File Transfer Protocol (FTP), Remote Copy Protocol (RCP), Secured Copy Protocol (SCP), Secured FTP (SFTP), or Trivial FTP (TFTP).

Table 1 describes the syntax for the *url* argument when saving the file to a remote server.

Table 1 Syntax for the url Argument in the save configuration Command

Server Protocol	URL Format
FTP, SCP, or SFTP	**ftp://***username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename.ext* **scp://***username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename.ext* **sftp://***username*[**:***passwd*]@{*ip-addr* | *hostname*}[//*directory*]/*filename.ext*

Table 1 Syntax for the url Argument in the save configuration Command

Server Protocol	URL Format
RCP	**rcp://***username***@**{*ip-addr* | *hostname*}[**//***directory*]**/***filename***.***ext*
TFTP	**ftp://**{*ip-addr* | *hostname*}[**//***directory*]**/***filename***.***ext*

You can specify the *hostname* argument only if Domain Name System (DNS) is enabled with the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see *Command List*.

Note: Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of username account home directory).

If you attempt to overwrite an existing file on the local file system, the system prompts you for confirmation. Use the **-noconfirm** optional keyword to replace an existing file without providing confirmation to the system. In either case, the system saves a backup of the existing file with the .bak file extension. Only a single copy of the file is saved as a backup.

1.5.6 Examples

The following example shows how to save the current active system configuration to a file, **current.cfg**, on the local file system. The user is prompted to overwrite an existing file:

```
[local]Redback#save configuration /flash/current.cfg



Save to file: current.cfg

Target file exists, overwrite? y
```

The following example shows that the existing **current.cfg** file has been saved as **current.cfg.bak:**

```
[local]Redback#directory /flash
```

```
Contents of /flash
total 2590
-rw-r--r--  1 root  10000     4564 Jan 23 2006  current.cfg
-rw-r--r--  1 root  10000     3654 Jan 23 2006  current.cfg.bak
-rw-r--r--  1 root  10000     1578 Jan 23 2006  redback.cfg
```

1.6 save log

save log [***text***] ***filename*** [**-noconfirm**]

1.6.1 Purpose

Saves one of the internal event log buffers to the flash file system.

1.6.2 Command Mode

Exec (10)

1.6.3 Syntax Description

text	Optional. Event log is saved in plain text. Default form is in binary if this argument is not specified.
filename	Name of the file to which log entries are to be saved. Local filename is specified. If the full path is not specified, the default directory is /flash.
-noconfirm	Optional. Overwrites the specified filename if it already exits without user confirmation.

1.6.4 Default

None

1.6.5 Usage Guidelines

Use the **save log** command to save one of the internal event log buffers to the flash file system for later examination.

To examine the debugging messages, use the **logging debug** command in global configuration mode; to save the messages prior to examining them, use the **save log** command. You can use the **logging filter** command in context configuration mode to specify different levels of logging filters.

For more information about the **logging debug** and **logging filter** commands, see *Command List*.

1.6.6 Examples

The following example shows how to save a copy of the log to the file, **log.sav**, in the **/flash** directory:

```
[local]Redback#save log log.sav
```

1.7 save seos-core

save seos-core

1.7.1 Purpose

Saves a previously written core dump of the operating system to the mass-storage device in the /md partition.

1.7.2 Command Mode

Exec (10)

1.7.3 Syntax Description

This command has no keywords or arguments.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **save seos-core** command to save a core dump, which the operating system kernel has previously written to the swap partition on the mass-storage device, to the /md partition on the same device; the SmartEdge router must have a mass-storage device installed to use this command.

Either controller card can detect a problem and cause its kernel to dump an image of the running operating system on its mass-storage device. When you enter this command, you must be using a command-line interface (CLI) running on that same controller card to allow the command to access the core dump in the swap partition. For example, if the controller card that wrote the core dump has become the standby controller after reloading the operating system, you must connect to the local console for the standby controller card; if it was the active controller card, you can access the CLI from either the local console or the management port. Logging messages identify the controller card that wrote the core dump to the swap partition.

This command saves the core dump in two crash files. The filenames for these files, netbsd.0.core.gz and netbsd.0.gz, are fixed; however, you can rename the files after the save operation is complete. If you rename the files, we recommend that you add only the date to the filenames to ensure that “core” remains in the filename for the netbsd.0.core.gz file.

Note: The files created by this command are useful only for the support organization when troubleshooting the problem that caused the core dump.

1.7.6 Examples

The following example shows how to save a core dump of the operating system to two crash files in the /md partition on the mass-storage device of the active controller card and rename them to include the date of the core dump:

```
[local]Redback#save seos-core

dumplo = 89128960 (174080 * 512)

savecore:  number read 512 value of magic on disk is 76910538

savecore: newdumpmag: 4958fca

savecore: dumpsize is 91003972

savecore: /md/bounds: No such file or directory

savecore: writing compressed core to /md/netbsd.0.core.gz

savecore: total output bytes(uncompressed):442499072

savecore: writing compressed kernel to /md/netbsd.0.gz

[local]Redback#rename /md/netbsd.0.core.gz /md/netbsd031002.0.core.gz

[local]Redback#rename /md/netbsd.0.gz /md/netbsd031002.0.gz
```

1.8 schema

schema ***sch-prof-name***

no schema ***sch-prof-name***

1.8.1 Purpose

Applies a system-level bulkstats schema profile to gather system-wide statistics using this policy.

1.8.2 Command Mode

Bulkstats configuration

1.8.3 Syntax Description

sch-prof-name	Name of the global schema profile. Alphanumeric string with up to 19 characters.

1.8.4 Default

None

1.8.5 Usage Guidelines

Use the **schema** command to apply a system-level (global) bulkstats schema profile to gather system-wide statistics using this policy. You can apply multiple schema profiles using this command. Each schema can gather a different type and format of data. Each application of a schema profile is used to create a text record that is appended to the bulkstats collection file for this policy after every sample period.

Caution!

Risk of system performance degradation. Although you can apply multiple schema profiles, each gathering a different type and format of data, it is advisable to minimize the number of schema profile applications to reduce impact on system performance. To reduce the risk, you can instead create one schema profile that records several subsets of data. Separate each subset within the format string by entering the **\n** character sequence, which creates a new starting line in the output file. You can then apply this single schema profile in place of multiple schema profiles.

Use the **no** form of this command to remove the specified schema profile.

1.8.6 Examples

The following example shows how to apply a previously configured schema profile **sample** for the **bulk** policy:

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

[local]Redback(config-ctx)#bulkstats policy bulk

[local]Redback(config-bulkstats)#schema sample
```

1.9 schema-dump

schema-dump

no schema-dump

1.9.1 Purpose

Enables writing the definitions of the configured bulkstats schema profiles to the beginning of the bulkstats data collection file.

1.9.2 Command Mode

Bulkstats configuration

1.9.3 Syntax Description

This command has no keywords or arguments.

1.9.4 Default

No schema profile definition is saved in any bulkstats data collection file for any policy.

1.9.5 Usage Guidelines

Use the **schema-dump** command to enable writing the definitions of the configured bulkstats schema profiles to the beginning of the bulkstats data collection file. When enabled, the definition of each configured schema profile is printed at the beginning of the bulkstats collection file.

Use the **no** form of this command to disable writing the definitions of schema profiles to the bulkstats data collection file.

1.9.6 Examples

The following example shows how to write the definitions of the configured bulkstats schema profiles to the bulkstats data file:

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

[local]Redback(config-ctx)#bulkstats policy bulk

[local]Redback(config-bulkstats)#schema-dump
```

1.10 scramble

scramble

{**no** | **default**} **scramble**

1.10.1 Purpose

Enables X^43+1 synchronous payload envelope (SPE) scrambling on a Packet over SONET/SDH (POS) port, as specified in RFC 2615, *PPP over SONET/SDH*.

1.10.2 Command Mode

Port configuration

1.10.3 Syntax Description

This command has no keywords or arguments.

1.10.4 Default

SPE scrambling is enabled on the port.

1.10.5 Usage Guidelines

Use the **scramble** command to enable X^43 +1 scrambling on a POS port, as specified in RFC 2615, `PPP over SONET/SDH`.

Note: Enabling or disabling scrambling on a port also changes the Path Label Signal (C2) byte value to the default specified in RFC 2615; see the **c2byte** command in port configuration mode.

Note: This command does not apply to Asynchronous Transfer Mode (ATM), Ethernet, or channelized OC-12 ports.

Note: The SmartEdge 100 router does not support POS ports.

Use the **no** form of this command to disable SPE payload scrambling.

Use the **default** form of this command to enable SPE payload scrambling.

1.10.6 Examples

The following example shows how to disable SPE scrambling for port **1** on the POS traffic card in slot **11**. It also results in the C2 value being set to the value of 0xCF:

```
[local]Redback(config)#port pos 11/1

[local]Redback(config-port)#no scramble
```

1.11 send

send {**permit** | **deny**}

no send {**permit** | **deny**}

1.11.1 Purpose

Configures the setting in the IGMP snooping profile that controls the ability of the associated circuits to send multicast data.

1.11.2 Command Mode

IGMP snooping profile configuration

1.11.3 Syntax Description

`permit`	Permits circuits to send multicast data.
`deny`	Denies sending multicast data by circuits.

1.11.4 Default

Sending multicast data is permitted on all circuits.

1.11.5 Usage Guidelines

Use the **send** command to configure the setting in the IGMP snooping profile that controls the ability of the associated circuits to send multicast data.

Use the **no** form of this command to return the IGMP snooping profile to the default setting in which sending multicast data is permitted on all circuits.

1.11.6 Examples

The following example shows how to deny sending multicast data by all circuits attached to an IGMP snooping profile called `sanjose1`:

```
[local]Redback#configure

[local]Redback(config)#igmp snooping profile sanjose1

[local]Redback(config-igmp-snooping-profile)#send deny
```

The following example shows how to permit sending multicast data by all circuits attached to an IGMP snooping profile called `sanjose1`:

```
[local]Redback#configure

[local]Redback(config)#igmp snooping profile sanjose1

[local]Redback(config-igmp-snooping-profile)#send permit
```

1.12 send community

send community

no send community

1.12.1 Purpose

Specifies that the community attribute is sent to the specified external Border Gateway Protocol (eBGP) neighbor or peer group.

1.12.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.12.3 Syntax Description

This command has no keywords or arguments.

1.12.4 Default

The community attribute is not sent to the eBGP neighbor or peer group. The community attribute is always sent to internal BGP (iBGP) peers.

1.12.5 Usage Guidelines

Use the **send community** command to specify that the community attribute is sent to the specified eBGP neighbor or peer group.

Note: This command is used only with eBGP neighbors or peer groups. The community attribute is always sent to iBGP peers.

Note: You cannot enable this command 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 **no** form of this command to restore the default behavior of not sending the community attribute to eBGP neighbors.

1.12.6 Examples

The following example shows how to send the community attribute to the eBGP neighbor at IP address **123.45.34.2:**

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

[local]Redback(config-bgp)#neighbor 123.45.34.2 external

[local]Redback(config-bgp-neighbor)#remote as-200

[local]Redback(config-bgp-neighbor)#send community
```

1.13 send ext-community

send ext-community

no send ext-community

1.13.1 Purpose

Specifies that the extended community attribute is sent to the specified external Border Gateway Protocol (eBGP) neighbor or peer group.

1.13.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.13.3 Syntax Description

This command has no keywords or arguments.

1.13.4 Default

The extended community attribute is not sent to the eBGP neighbor or peer group. The extended community attribute is always sent to internal BGP (iBGP) peers.

1.13.5 Usage Guidelines

Use the **`send ext-community`** command to specify that the extended community attribute is sent to the specified eBGP neighbor or peer group.

Note: This command is used only with eBGP neighbors or peer groups. The extended community attribute is always sent to iBGP peers.

Note: You cannot enable this command 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 **`no`** form of this command to restore the default behavior of not sending the extended community attribute to eBGP neighbors.

1.13.6 Examples

The following example shows how to send the extended community attribute to the eBGP neighbor at IP address **123.45.34.2:**

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

[local]Redback(config-bgp)#neighbor 123.45.34.2 external

[local]Redback(config-bgp-neighbor)#remote as-200

[local]Redback(config-bgp-neighbor)#send ext-community
```

1.14 send filter prefix-list

`send filter prefix-list`

`no send filter prefix-list`

1.14.1 Purpose

Advertises to a Border Gateway Protocol (BGP) peer that a BGP speaker can send prefixed-based filtering to a peer.

1.14.2 Command Mode

BGP neighbor configuration

1.14.3 Syntax Description

This command has no keywords or arguments.

1.14.4 Default

The command is disabled.

1.14.5 Usage Guidelines

Use the **`send filter prefix-list`** command to advertise to a BGP peer that a BGP speaker can send address prefix-based route filtering to a peer.

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

Use this command to save resources and avoid the generation, transmission, and processing of unnecessary routing updates.

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-addr`* **`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.

1.14.6 Examples

The following example shows how to enable the external BGP (eBGP) speaker at IP address, **10.1.1.1**, to send outbound route filters to BGP peers:

```
[local]Redback(config-bgp)#neighbor 10.1.1.1 external

[local]Redback(config-bgp-neighbor)#send filter prefix-list
```

1.15 send join

send join

no send join

1.15.1 Purpose

Sends join messages upstream on the RPF primary and secondary interface without any outgoing interfaces (OIFs) being present.

1.15.2 Command Mode

Pim-dual configuration

1.15.3 Syntax Description

This command has no keywords or arguments.

1.15.4 Default

The send-join feature is disabled for a group, and the SmartEdge router continues sending new join messages upstream in the network.

1.15.5 Usage Guidelines

Use the **send-join** command to send join messages upstream on the RPF primary and secondary interface without any OIFs being present. If a join message from IGMP is received by PIM after the send-join feature is enabled for a specific group, the SmartEdge router does not send any new join messages upstream in the network. Instead, the SmartEdge router immediately adds the client to the OIF list and starts forwarding the multicast stream. In other words, PIM sends the join messages upstream only once and maps the join from IGMP to PIM.

Use the **no** form of this command to disable sending join messages before any multicast receivers are present.

1.15.6 Examples

The following example shows how to enable the send-join feature on the group with an IP address of 255.100.1.1. With this configuration, PIM sends new join messages upstream only once and maps the join from IGMP to PIM:

```
[local]Redback(config-ctx)#pim dual-join group 225.100.1.1 source 192.110.30.6
[local]Redback(config-pim-dual)#send join
```

1.16 send label

send label

no send label

1.16.1 Purpose

Enables a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP IP Version 4 (IPv4) or IP Version 6 (IPv6) routes to a peer BGP router.

1.16.2 Command Mode

BGP neighbor address family configuration

1.16.3 Syntax Description

This command has no keywords or arguments.

1.16.4 Default

BGP routers distribute BGP IPv4 unicast routes without MPLS labels.

1.16.5 Usage Guidelines

Use the **send label** command to enable a BGP router to send MPLS labels with BGP IPv4 or IPv6 routes to a peer BGP router.

Note: You must configure this command on both the local router and the peer router in order for the routers to send IPv4 unicast or IPv6 unicast routes with MPLS labels.

One application for this command is the BGP/MPLS Virtual Private Network (VPN) Carrier Supporting Carrier configuration. The user must configure this command on the provider edge (PE) and customer edge (CE) routers between the super carrier and the ISP carrier.

This command has the following restrictions:

- If the **send label** command is configured for a peer that is already up, the BGP session with that peer will be automatically reset to make the configuration effective.
- The **send label** command is available only in the local and VPN contexts. In the local context, the **send label** command is available in iBGP and eBGP peer configurations. In VPN contexts, the **send label** command is available in eBGP peer configurations.
- The **send label** command transports IPv6 routes only if MPLS is enabled on the IPv4 core.
- The **send label** command is supported for unicast address families only.
- The **send label** command is available only in the local and VPN contexts.

Use the **no** form of this command to disable the BGP router from sending MPLS labels with IPv4 unicast routes.

1.16.6 Examples

The following example shows how to enable the local router to send MPLS labels along with BGP IPv4 unicast routes to peer **1.1.1.1:**

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

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

[local]Redback(config-bgp)#neighbor 1.1.1.1 external

[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast

[local]Redback(config-bgp-peer-af)#send label
```

The following example shows how to enable the local router to send MPLS labels along with BGP IPv6 routes to peer `1.1.1.1:`

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 1.1.1.1 external
[local]Redback(config-bgp-neighbor)#address-family ipv6 unicast
[local]Redback(config-bgp-peer-af)#send label
```

1.17 send-lifetime

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

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

1.17.1 Purpose

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

1.17.2 Command Mode

key chain configuration

1.17.3 Syntax Description

start-datetime	Date and time to start sending 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 Section 1.17.5 on page 23.
duration *seconds*	Optional. Number of seconds to continue sending the key. The range of values is 1 to 2147483646.
infinite	Optional. Specifies that the key is to be sent indefinitely.
stop-datetime	Optional. Date and time to stop sending 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 Section 1.17.5 on page 23.

1.17.4 Default

If you do not use this command, the key is sent starting immediately and continues to be sent indefinitely. If you do not specify a duration when using this command, the key is sent indefinitely.

1.17.5 Usage Guidelines

Use the **`send-lifetime`** command to specify when the key being configured is to be sent. 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, 2001).

- ***`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`*** = The second of the minute in two digits (for example, 55). The range of values is 0 to 59.

If you issue the **`send-lifetime`** command without any optional constructs, the key is sent starting with the date and time that you specify and continues to be sent indefinitely.

You can replace an existing send lifetime value by issuing the **`send-lifetime`** command again, and specifying new parameters.

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

1.17.6 Examples

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

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

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

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

1.18 send-mac-flush

`send-mac-flush`

1.18.1 Purpose

Enables a hub VPLS PE that transitions from standby to active mode to send a MAC withdrawal message to all peers.

1.18.2 Command Mode

VPLS configuration

1.18.3 Syntax Description

This command has no keywords or arguments.

1.18.4 Default

When a hub VPLS PE transitions from standby to active mode, it does not send a MAC withdrawal message to its peers.

1.18.5 Usage Guidelines

Use the **`send-mac-flush`** command to enable a hub VPLS that transitions from standby to active mode to send a MAC withdrawal message to its peers.

Use the **`no`** form of this command to disable the hub VPLS from sending MAC withdrawal messages to its peers.

1.18.6 Examples

The following example shows how to enable a hub VPLS PE that transitions from standby to active mode to send a MAC withdrawal message to all peers.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge headquarters
[local]Redback(config-bridge)#vpls
[local]Redback (config-vpls)#send-mac-flush
```

1.19 seq (Macro)

`seq` ***`num command-string`*** [***`param-num`***]...

```
no seq num
```

1.19.1 Purpose

Specifies a command in the macro.

1.19.2 Command Mode

Macro configuration

1.19.3 Syntax Description

num	Sequence number that denotes the order in which this command is included in the macro.
command-string	Command with the appropriate keywords, arguments, and constructs to be included in the macro. Use the $ symbol as a placeholder in the *command-string* argument to designate the arguments for the command.
param-num	Optional. Sequence number of a parameter to be entered with the macro name. Separate the sequence numbers with a space. The range of values is 1 to 10; the asterisk (*) character is also supported.

1.19.4 Default

No commands are specified for a macro.

1.19.5 Usage Guidelines

Use the **seq** command to specify a command to be included in the macro.

Use $1, $2, and so on, as placeholders in the *command-string* argument to designate the arguments for the command. You can specify up to nine placeholders, $1 to $9, for command arguments. Use the asterisk (*) character to specify all values of that argument for the command.

Use the **exit** command in macro configuration mode to complete the macro and exit to global configuration mode.

Use the **no** form of this command to delete the command from the macro.

1.19.6 Examples

The following example shows how to define the macro, **show-all-port**, to display port information:

```
[local]Redback(config)#macro inherit show-port-all
[local]Redback(config-macro)#seq 10 show port $1/$2
[local]Redback(config-macro)#seq 20 show circuit $1/$2
[local]Redback(config-macro)#exit
```

The following example displays port and circuit data for port **3** of the traffic card in slot **4** using the same macro:

```
[local]Redback#show-port-all 4 3
```

The following example shows how to define a macro that uses the * character:

```
[local]Redback(config)#macro inherit show-all
[local]Redback(config-macro)#seq 10 show config $*
[local]Redback(config-macro)#seq 20 show ip interface $*
[local]Redback(config-macro)#seq 30 show circuit $*
[local]Redback(config-macro)#exit
```

The following example shows how to capture the information displayed by the same macro in the file, **output.txt:**

```
[local]Redback#show-all | append output.txt
```

1.20 seq (IPv4 ACL)

Statements in IPv4 and IPv6 ACLs can contain different criteria; for syntax for statements in IPv6 ACLs, see seq (IPv6 ACL).

seq {**permit** | **deny**} [*protocol*] {*src src-wildcard* | **any** | **host** *src*} [{*cond port* | **range** *port end-port*}] [**max-sessions** *limit*] [**min-sessions** *limit*] [**dest** *dest-wildcard* | **any** | **host** *dest*] [*cond port* | **range** *port end-port*] [**length** {*cond length* | **range** *length end-length*}] [**icmp-type** *icmp-type* [**icmp-code** *icmp-code*]] [**igmp-type** *igmp-type*] [**dscp eq** *dscp-value*] [**established**] [**precedence** *prec-value*] [**tos** *tos-value*] [**class** *class-name*] [**condition** *cond-id*]

no permit *src src-wildcard*

1.20.1 Purpose

Creates an IPv4 access control list (ACL) statement that denies or allows packets that meet the specified criteria and sets the order of the statement in the ACL.

1.20.2 Command Mode

Access control list configuration

1.20.3 Syntax Descriptions

`seq-num`	Sequence number for the statement in an ACL. The range of values is 1 to 4,294,967,295.
`deny`	Deny packets with the specified criteria.
`permit`	Allow packets with the specified criteria
`protocol`	Optional. Number indicating a supported protocol as specified in RFC 1700, *Assigned Numbers* . The range of values is 0 to 255 or one of the keywords listed in Table 2.
`src`	Source address to be included in the permit or deny criteria; an IP address in the form *`A.B.C.D`*.
`src-wildcard`	Indication of which bits in the *`src`* argument are significant for purposes of matching; expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the *`src-wildcard`* argument must be matched by the corresponding bits in the *`src`* argument. For any one-bits in the *`src-wildcard`* argument, the corresponding bits in the *`src`* argument are ignored.
`any`	Specifies a completely wildcard source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.
`host` *`src`*	Address of a single-host source with no wildcard address bits. The `host` *`source`* construct is identical to the *`src src-wildcard`*construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
`cond`	Optional. Matching condition for the *`port`* or *`length`* argument, according to one of the keywords listed in Table 3.
`port`	Optional. TCP or UDP source or destination port. This argument is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 4 and Table 5.
`range` *`port end-port`*	Optional if you specify the TCP or UDP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must be within the specified range to match the criteria. The range of values is 1 to 65,535 or one of the keywords listed in Table 4 and Table 5. Available with the `seq permit` construct only.
`max-sessions` *`limit`*	Optional. Maximum number of sessions allowed for the specified IP address or IP subnet. This construct is only available for TCP. Use the `ip access-list` command with the `ssh-and-telnet-acl` keyword to apply an IP ACL to packets associated with an Secured Shell (SSH) or a Telnet server. The range of values is 1 to 32. Available with the `seq permit` construct only.

min-sessions *limit*	Optional. Minimum number of sessions allowed for the specified IP address or IP subnet. This construct is only available if you specify TCP as the protocol in this command and use the ip access-list command with the ssh-and-telnet-acl keyword to apply an IP ACL to packets associated with an SSH or a Telnet server. The range of values is 0 to 32. The sum of values specified for the min-sessions *limit* construct for all specified IP addresses or IP subnets must not exceed 32.
dest	Optional. Destination address to be included in the permit or deny criteria; an IP address in the form *A.B.C.D*.
dest-wildcard	Indication of which bits in the *dest* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *dest-wildcard* argument mean that the corresponding bits in the *dest* argument must match; one-bits in the *dest-wildcard* argument mean that the corresponding bits in the *dest* argument are ignored.
host *dest*	Address of a single-host destination with no wildcard address bits. The host *dest* construct is identical to the *dest dest-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
length	Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header, regardless of the specified protocol.
length	Packet length. The range of values is 20 to 65,535.
range *length end-length*	Packets that fall into the range of specified lengths. Each value (*length* and *end-length*) can be from 20 to 65,535.
icmp-type *icmp-type*	Optional. Type of ICMP packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 6. This argument is only available if you specify icmp for the *protocol* argument.
icmp-code *icmp-code*	Optional if you use the icmp-type*icmp-type* construct. A particular ICMP message code to be matched. The range of values is 0 to 255. This argument is only accepted if you specified icmp for the *protocol* argument.
igmp-type *igmp-type*	Optional. Type of IGMP packet to be matched. This argument is only accepted if you specified igmp as the *protocol* argument. The range of values is 0 to 15 or one of the keywords listed in Table 7.
dscp eq *dscp-value*	Optional. Packet Differentiated Services Code Point (DSCP) value must be equal to the value specified in the *dscp-value* argument to match the criteria. The range of values is 0 to 63 or one of the keywords listed in Table 8.
established	Optional. Specifies that only established connections are to be matched. This keyword is only available if you specify tcp for the *protocol* argument.
precedence *prec-value*	Optional. Precedence value of packets to be considered a match. The range of values is 0 to 7, 7 being the highest precedence, or one of the keywords listed in Table 9.
tos *tos-value*	Optional. Type of service (ToS) to be considered a match. The range of values is 0 to 15 or one of the keywords listed in Table 10.
class*class-name*	Optional. Policy-based class name. Available with the seq permit construct in policy ACLs only.
condition *cond-id*	Optional. ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295.

1.20.4 Default

None

1.20.5 Usage Guidelines

Use the **seq deny** and **seq permit** constructs to create IP ACL statements to deny or allow packets that meet the specified criteria. This command also sets the order of the statement in the ACL. You can also use the **deny** and **permit** commands to create IP ACL statements; in this case, the SmartEdge OS automatically sets the order of the statement in the ACL (seq 10, seq 20, seq 30, and so forth in the order they were configured).

In the IPv4 syntax, the *cond port* and *cond length* constructs are mutually exclusive with the **range** *port end-port* and **range** *length end-length* constructs.

With the **seq permit** construct, you can use the optional **max-sessions** *limit* and **min-sessions** *limit* constructs to specify a maximum or minimum number of simultaneous SSH or Telnet sessions allowed from an IP address or subnet. These constructs are available if you use the **service ssh server** or **service telnet server** commands with the **access-group** keyword to enable the SSH or Telnet protocol and apply the ACL. For statements where the **any** keyword is specified for both source and destination, only the **max-sessions limit** construct applies.

Note: In all ACLs, there is an automatic **deny any any** statement at the end of the list. This implicit statement could block valid access to a context; for example, in the local context, it could block administrator access to the Ethernet management port. To allow administrator access, add a statement to allow access from authorized sources to the end of the list. For example, you could add a **seq** *seq-num* **permit ip any any** or **seq** *seq-num* **permit ip** *src src-wildcard dest dest-wildcard* statement to the ACL.

Use the **no** form of this command to delete the statement with the specified sequence number from the ACL.

You can use the *resequence ip access-list* command in context configuration mode to reorder the sequence of an ACL.

Table 11 lists the valid keyword values for the *protocol* argument:

Table 2 Valid Keyword Values for the protocol Argument

Keyword	Definition
ahp	Authentication Header Protocol
esp	Encapsulation Security Payload
gre	Generic Routing Encapsulation
host	Host source address
icmp	Internet Control Message Protocol
igmp	Internet Group Management Protocol

Table 2 Valid Keyword Values for the protocol Argument

Keyword	Definition
`ip`	Any IP protocol
`ipinip`	IP-in-IP tunneling
`ospf`	Open Shortest Path First
`pcp`	Payload Compression Protocol
`pim`	Protocol Independent Multicast
`tcp`	Transmission Control Protocol
`udp`	User Datagram Protocol

Table 3 lists the valid keyword values for the *`cond`* argument.

Table 3 Valid Keyword Values for the cond Argument

Keyword	Description
`eq`	Equal to
`gt`	Greater than
`lt`	Less than
`neq`	Not equal to

Table 13 lists the valid keyword values for the *`port`* argument when it is used to specify a TCP port.

Table 4 Valid Keyword Values for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`bgp`	Border Gateway Protocol (BGP)	179
`chargen`	Character generator	19
`cmd`	Remote commands (rcmd)	514
`daytime`	Daytime	13
`discard`	Discard	9
`domain`	Domain Name System	53
`echo`	Echo	7
`exec`	Exec (rsh)	512
`finger`	Finger	79
`ftp`	File Transfer Protocol	21
`ftp-data`	FTP data connections (used infrequently)	20

Table 4 Valid Keyword Values for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`gopher`	Gopher	70
`hostname`	Network interface card (NIC) hostname server	101
`ident`	Identification protocol	113
`irc`	Internet Relay Chat	194
`klogin`	Kerberos login	543
`kshell`	Kerberos Shell	544
`login`	Login (rlogin)	513
`lpd`	Printer service	515
`nntp`	Network News Transport Protocol	119
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`pop2`	Post Office Protocol Version 2	109
`pop3`	Post Office Protocol Version 3	110
`shell`	Remote command shell	514
`smtp`	Simple Mail Transport Protocol	25
`ssh`	Secure Shell	22
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`telnet`	Telnet	23
`time`	Time	37
`uucp`	UNIX-to-UNIX Copy Program	540
`whois`	Nickname	43
`www`	World Wide Web (HTTP)	80

Table 14 lists the valid keyword values for the *`port`* argument when it is used to specify a UDP port.

Table 5 Valid Keyword Values for the port Argument (UDP Port)

Keyword	Definition	Corresponding Port Number
`biff`	Biff (Mail Notification, Comsat)	512
`bootpc`	Bootstrap Protocol client	68
`bootps`	Bootstrap Protocol server	67
`discard`	Discard	9
`dnsix`	DNSIX Security Protocol Auditing	195
`domain`	Domain Name System	53
`echo`	Echo	7
`isakmp`	Internet Security Association and Key Management Protocol (ISAKMP)	500
`mobile-ip`	Mobile IP Registration	434
`nameserver`	IEN116 Name Service (obsolete)	42
`netbios-dgm`	NetBIOS Datagram Service	138
`netbios-ns`	NetBIOS Name Service	137
`netbios-ss`	NetBIOS Session Service	139
`ntp`	Network Time Protocol	123
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`rip`	Router Information Protocol (router, in.routed)	520
`snmp`	Simple Network Management Protocol	161
`snmptrap`	SNMP Traps	162
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`tftp`	Trivial File Transfer Protocol	69
`time`	Time	37
`who`	Who Service (rwho)	513
`xdmcp`	X Display Manager Control Protocol	177

Table 15 lists the valid keyword values for the *`icmp-type`* argument.

Table 6 Valid Keyword Values for the icmp-type Argument

Keyword	Description
`administratively-prohibited`	Administratively prohibited
`alternate-address`	Alternate address
`conversion-error`	Datagram conversion
`dod-host-prohibited`	Host prohibited
`dod-net-prohibited`	Net prohibited
`echo`	Echo (ping)
`echo-reply`	Echo reply
`general-parameter-problem`	General parameter problem
`host-isolated`	Host isolated
`host-precedence-unreachable`	Host unreachable for precedence
`host-redirect`	Host redirect
`host-tos-redirect`	Host redirect for ToS
`host-tos-unreachable`	Host unreachable for ToS
`host-unknown`	Host unknown
`host-unreachable`	Host unreachable
`information-reply`	Information replies
`information-request`	Information requests
`log`	Log matches against this entry
`log-input`	Log matches against this entry, including input interface
`mask-reply`	Mask replies
`mask-request`	Mask requests
`mobile-redirect`	Mobile host redirects
`net-redirect`	Network redirect
`net-tos-redirect`	Network redirect for ToS
`net-tos-unreachable`	Network unreachable for ToS
`net-unreachable`	Network unreachable
`network-unknown`	Network unknown
`no-room-for-option`	Parameter required but no room
`option-missing`	Parameter required but not present
`packet-too-big`	Fragmentation needed and DF set

Table 6   Valid Keyword Values for the icmp-type Argument

Keyword	Description
`parameter-problem`	All parameter problems
`port-unreachable`	Port unreachable
`precedence`	Match packets with given precedence value
`precedence-unreachable`	Precedence cutoff
`protocol-unreachable`	Protocol unreachable
`reassembly-timeout`	Reassembly timeout
`redirect`	All redirects
`router-advertisement`	Router discovery advertisement
`router-solicitation`	Router discovery solicitation
`source-quench`	Source quenches
`source-route-failed`	Source route failed
`time-exceeded`	All time exceeded messages
`time-range`	Specify a time-range
`timestamp-reply`	Timestamp replies
`timestamp-request`	Timestamp requests
`tos`	Match packets with given type of service (ToS) value
`traceroute`	Traceroute
`ttl-exceeded`	TTL Exceeded
`unreachable`	All unreachables

Table 7 lists the valid keyword values for the *`igmp-type`* argument.

Table 7   Valid Keyword Values for the igmp-type Argument

Keyword	Description
`dvmrp`	Specifies Distance-Vector Multicast Routing Protocol.
`Host-query`	Specifies host query.
`Host-report`	Specifies host report.
`pim`	Specifies Protocol Independent Multicast.

Table 8 lists the valid keyword values for the *`dscp-value`* argument.

Table 8 Valid Keyword Values for the dscp-value Argument

Keyword	Definition
`af11`	Assured Forwarding—Class 1/Drop precedence 1
`af12`	Assured Forwarding—Class 1/Drop precedence 2
`af13`	Assured Forwarding—Class 1/Drop precedence 3
`af21`	Assured Forwarding—Class 2/Drop precedence 1
`af22`	Assured Forwarding—Class 2/Drop precedence 2
`af23`	Assured Forwarding—Class 2/Drop precedence 3
`af31`	Assured Forwarding—Class 3/Drop precedence 1
`af32`	Assured Forwarding—Class 3/Drop precedence 2
`af33`	Assured Forwarding—Class 3/Drop precedence 3
`af41`	Assured Forwarding—Class 4/Drop precedence 1
`af42`	Assured Forwarding—Class 4/Drop precedence 2
`af43`	Assured Forwarding—Class 4/Drop precedence 3
`cs0`	Class Selector 0
`cs1`	Class Selector 1
`cs2`	Class Selector 2
`cs3`	Class Selector 3
`cs4`	Class Selector 4
`cs5`	Class Selector 5
`cs6`	Class Selector 6
`cs7`	Class Selector 7
`df`	Default Forwarding (same as cs0)
`ef`	Expedited Forwarding

Table 9 lists the valid keyword values for the ***`prec-value`*** argument.

Table 9 Valid Keyword Values for the prec-value Argument

Keyword	Description
`tine`	Specifies routine precedence (value=0).
`priority`	Specifies priority precedence (value=1).
`immediate`	Specifies immediate precedence (value=2).
`flash`	Specifies flash precedence (value=3).
`flash-override`	Specifies flash override precedence (value=4).
`critical`	Specifies critical precedence (value=5).

Table 9 Valid Keyword Values for the prec-value Argument

Keyword	Description
`internet`	Specifies internetwork control precedence (value=6).
`network`	Specifies network control precedence (value=7).

Table 10 lists the valid keyword values for the ***tos-value*** argument.

Table 10 Valid Keyword Values for the tos-value Argument

Keyword	Description
`max-reliability`	Specifies maximum reliable ToS (value=2).
`max-throughput`	Specifies maximum throughput ToS (value=4).
`min-delay`	Specifies minimum delay ToS (value=8).
`min-monetary-cost`	Specifies minimum monetary cost ToS (value=1).
`normal`	Specifies normal ToS (value=0).

1.20.6 Examples

The following example shows how to specify that all IP traffic to destination host, **10.25.1.1**, is to be denied, and all other traffic on subnet **10.25.1/24** is to be permitted:

```
[local]Redback(config-ctx)#ip access-list protect201
[local]Redback(config-access-list)#seq 12 deny ip any host 10.25.1.1
[local]Redback(config-access-list)#seq 22 permit ip any 10.25.1.0 0.0.0.255
```

1.21 seq (IPv6 ACL)

Statements in IPv4 and IPv6 ACLs can contain different criteria; for syntax for statements for IPv4 ACLs, see seq (IPV4 ACL).

seq ***seq-num*** {**deny** | **permit**} [***protocol***] {***src-ipv6-addr/prefix-length*** | **any** } [***cond***] [**range** ***port end-port***] [***dest-ipv6-addr/prefix-length*** | **any**] [**icmp-type** ***icmp-type***] [**icmp-code** ***icmp-code***]] [**established**] [**traffic-class eq** ***traffic-class-value***] [**condition** ***cond-id***]

no seq ***seq-num***

1.21.1 Command Mode

Access control list configuration

1.21.2 Syntax Descriptions

seq-num	Sequence number for the statement in an ACL. The range of values is 1 to 4,294,967,295.
deny	Deny packets with the specified criteria.
permit	Allow packets with the specified criteria.
protocol	Optional. Number indicating a supported protocol as specified in RFC 1700, *Assigned Numbers*. The range of values is 0 to 255 or one of the keywords listed in: For statements in IPv6 ACLs, see Table 11.
src-ipv6-address /prefix-length **any**	The traffic source to add to the statement criteria. The *src-ipv6-address* argument is in the format A:B:C:D::E/*prefix-length*, where the prefix length can be from 0 to 128. Indicates that IP traffic to or from all IP addresses is to be included in the **permit** or **deny** criteria.
cond	Required if you specify the TCP or UDP protocol. Matching condition according to one of the keywords listed in Table 12.
range *port end-port*	Optional if you specify the TCP or UCP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must be within the specified range to match the criteria. The range of values is 1 to 65,535 or one of the keywords listed in Table 13 and Table 14.
dest-ipv6-addr/prefix-length	The traffic destination to be matched. The *src-ipv6 -address/prefix-length* argument is in the format *A:B:C:D::E/prefix-length*, where the range of values for the prefix length can be from 0 to 128.
icmp-type *icmp-type*	Optional. Type of ICMP packet to be matched. The range of values is 0 to 255, or one of the keywords listed in Table 15. This argument is only available if you specify **icmp** for the *protocol* argument.
icmp-code *icmp-code*	Optional if you use the **icmp-type** *icmp-type* construct. A particular ICMP message code to be matched. The range of values is 0 to 255.
established	Optional with the TCP protocol. Specifies that only established TCP port connections are to be matched. This keyword is only available if you specify **tcp** for the *protocol* argument.

traffic eq *traffic-class-value*	Optional. Type of traffic class to be matched. The *traffic-class-value* argument is a DSCP; the range of values is from 0 to 63 or one of the DSCP keywords in Table 16.
condition *cond-id*	Optional. Matching ACL condition ID, in integer or IP address format. The ID range of values is 1 to 4,294,967,295. Not supported with IPv6 administrative ACLs applied to the Ethernet management port; conditions are ignored on that port.

1.21.3 Default

None

1.21.4 Usage Guidelines

The **seq deny** and **seq permit** constructs create an IPv6 access control list (ACL) statement that denies or allows packets that meet the specified criteria

This command also sets the order of the statement in the ACL. You can also use the *deny* and *permit* commands to create an IP ACL statement; in this case, the SmartEdge OS automatically sets the order of the statement in the ACL.

For IPv6s, the recommended limit is 100 rules for each IPv6 ACL.

Note: In all ACLs, there is an automatic **deny any any** statement at the end of the list. This statement could block valid access to a context, but would not appear in the output of the **show configuration acl** command. For example, in the local context, it could block administrator access to the Ethernet management port. To allow administrator access, add a statement to allow access from authorized sources to the end of the list. For example, you could add a **seq** *seq-num* **permit ipv6 any any** or **seq** *seq-num* **permit ipv6** *src src-wildcard dest dest-wildcard* statement to the ACL.

IPv6 administrative ACLs in contexts also have an implicit statement that enables IPv6 Neighbor Discovery.

Use the **no** form of this command to delete the statement with the specified sequence number from the ACL.

You can use the *resequence ip access-list* command in context configuration mode to reorder the sequence of an ACL.

Table 11 lists the valid keyword values for the *protocol* argument:

Table 11 *Valid Keyword Values for the protocol Argument*

icmp	ICMP version 6; requires the IPv6 source prefix in the format 1:2:3:4:5:6:7::8/48 or the **any** keyword.
ipv6	Any IPv6 Protocol (excluding IPv6 extension headers). Requires the IPv6 source prefix in the format 1:2:3:4:5:6:7::8/48 or the **any** keyword.
ospf	Open Shortest Path First.
pcp	Payload Compression Protocol
pim	Protocol Independent Multicast.
tcp	Transmission Control Protocol.
udp	User Datagram Protocol.

Table 12 lists the valid keyword values for the ***cond*** argument.

Table 12 *Valid Keyword Values for the cond Argument*

Keyword	Description
eq	Equal to
gt	Greater than
lt	Less than
neq	Not equal to

Table 13 lists the valid keyword values for the ***port*** argument when it is used to specify a TCP port.

Table 13 *Valid Keyword Values for the port Argument (TCP Port)*

Keyword	Definition	Corresponding Port Number
bgp	Border Gateway Protocol (BGP)	179
chargen	Character generator	19
cmd	Remote commands (rcmd)	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name System	53
echo	Echo	7
exec	Exec (rsh)	512
finger	Finger	79
ftp	File Transfer Protocol	21

Table 13 Valid Keyword Values for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`ftp-data`	FTP data connections (used infrequently)	20
`gopher`	Gopher	70
`hostname`	Network interface card (NIC) hostname server	101
`ident`	Identification protocol	113
`irc`	Internet Relay Chat	194
`klogin`	Kerberos login	543
`kshell`	Kerberos Shell	544
`login`	Login (rlogin)	513
`lpd`	Printer service	515
`nntp`	Network News Transport Protocol	119
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`pop2`	Post Office Protocol Version 2	109
`pop3`	Post Office Protocol Version 3	110
`shell`	Remote command shell	514
`smtp`	Simple Mail Transport Protocol	25
`ssh`	Secure Shell	22
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`telnet`	Telnet	23
`time`	Time	37
`uucp`	UNIX-to-UNIX Copy Program	540
`whois`	Nickname	43
`www`	World Wide Web (HTTP)	80

Table 14 lists the valid keyword values for the *`port`* argument when it is used to specify a UDP port.

Table 14   Valid Keyword Values for the port Argument (UDP Port)

Keyword	Definition	Corresponding Port Number
`biff`	Biff (Mail Notification, Comsat)	512
`bootpc`	Bootstrap Protocol client	68
`bootps`	Bootstrap Protocol server	67
`discard`	Discard	9
`dnsix`	DNSIX Security Protocol Auditing	195
`domain`	Domain Name System	53
`echo`	Echo	7
`isakmp`	Internet Security Association and Key Management Protocol (ISAKMP)	500
`mobile-ip`	Mobile IP Registration	434
`nameserver`	IEN116 Name Service (obsolete)	42
`netbios-dgm`	NetBIOS Datagram Service	138
`netbios-ns`	NetBIOS Name Service	137
`netbios-ss`	NetBIOS Session Service	139
`ntp`	Network Time Protocol	123
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`rip`	Router Information Protocol (router, in.routed)	520
`snmp`	Simple Network Management Protocol	161
`snmptrap`	SNMP Traps	162
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`tftp`	Trivial File Transfer Protocol	69
`time`	Time	37
`who`	Who Service (rwho)	513
`xdmcp`	X Display Manager Control Protocol	177

Table 15 lists the valid keyword values for the ***icmp-type*** argument.

Table 15 Valid Keyword Values for the icmp-type Argument

Keyword	**Description**
`destination-unreachable`	Destination-unreachable message
`echo-reply`	Echo reply message
`echo-request`	Echo request message
`mipv6`	Mobile IPv6 message; can be: • ha-address-reply (Home Agent Address Reply) • ha-address request (Home Agent Address Request) • prefix-advertisement (Mobile Prefix Advertisement) • prefix-solicitation (Mobile Prefix Solicitation)
`mld`	Multicast Listener Discovery
`nd`	Neighbor Discovery message; can be: • neighbor-advertisement (ND advertisement) • neighbor-solicitation (ND solicitation) • redirect (ND redirect message) • router-advertisement (ND router advertisement) • router-solicitation (ND router solicitation)
`packet-too-big`	Fragmentation needed and DF set
`parameter-problem`	All parameter problems
`renumbering`	Router renumbering message
`send`	Secure Neighbor Discovery messages; can be: • path-advertisement (Certification Path Advertisement) • path-solicitation (Certification Path Solicitation)
`time-exceeded`	All time exceeded messages

Table 16 lists the valid keyword values for the ***traffic-class-value*** argument.

Table 16   Valid Keyword Values for the traffic-class-value (DSCP) Argument

Keyword	Definition
`af11`	Assured Forwarding—Class 1/Drop precedence 1
`af12`	Assured Forwarding—Class 1/Drop precedence 2
`af13`	Assured Forwarding—Class 1/Drop precedence 3
`af21`	Assured Forwarding—Class 2/Drop precedence 1
`af22`	Assured Forwarding—Class 2/Drop precedence 2
`af23`	Assured Forwarding—Class 2/Drop precedence 3
`af31`	Assured Forwarding—Class 3/Drop precedence 1
`af32`	Assured Forwarding—Class 3/Drop precedence 2
`af33`	Assured Forwarding—Class 3/Drop precedence 3
`af41`	Assured Forwarding—Class 4/Drop precedence 1
`af42`	Assured Forwarding—Class 4/Drop precedence 2
`af43`	Assured Forwarding—Class 4/Drop precedence 3
`cs0`	Class Selector 0
`cs1`	Class Selector 1
`cs2`	Class Selector 2
`cs3`	Class Selector 3
`cs4`	Class Selector 4
`cs5`	Class Selector 5
`cs6`	Class Selector 6
`cs7`	Class Selector 7
`df`	Default Forwarding (same as cs0)
`ef`	Expedited Forwarding

1.21.5 Examples

The following example shows how to deny TCP traffic with the prefix 22:1:1::2/128 with default forwarding (DSCP code df) and all UDP traffic from port 80 or 81, and permit all IPv6 traffic:

```
[local]Redback(config-ctx)#ipv6 access-list listmgt
[local]Redback(config-access-list)#seq 21 deny tcp 22:1:1::2/128 any traffic-class eq df
[local]Redback(config-access-list)#seq 31 deny udp any any range 80 81
[local]Redback(config-access-list)#seq 41 permit ipv6 any any
```

1.22 server

server *ip-addr* **[prefer] [source** *if-name***] [version** *num***]**

{**no** | **default**} **server** *ip-addr* **[prefer] [source** *if-name***] [version** *num***]**

1.22.1 Purpose

Configures the NTP server for a context.

1.22.2 Command Mode

NTP server configuration

1.22.3 Syntax Description

ip-addr	IP address of the NTP server.
prefer	Configures this server as preferred to provide synchronization.
source *if-name*	Interface name for outgoing NTP messages; the interface connected to the subnet for NTP broadcasting. The default is the outgoing interface.
version *num*	NTP version to be used; can be 1-3. The default is 3.

1.22.4 Default

There is no NTP server enabled in the context.

1.22.5 Usage Guidelines

To allow the system clock to be synchronized to an authoritative time source, configure an NTP server in a context with the **server** command. To name the NTP broadcast interface (connected to the subnet served by this NTP server), use the **source** *if-name* construct.

To disable the NTP server, use the **no** form of the command.

1.22.6 Examples

The following example shows how to configure an NTP server for the ips202 context.

```
[local]Redback(config)#context isp202
[local]Redback(config-ctx)#ntp-mode
[local]Redback(config-ntp-server)#server-mode
[local]Redback(config-ntp-server)#server 1.1.1.2
prefer source ntp
```

1.23 server-group (DHCP)

server-group ***group-name***

no server-group

1.23.1 Purpose

Assigns a Dynamic Host Configuration Protocol (DHCP) server to a DHCP server group.

1.23.2 Command Mode

DHCP relay server configuration

1.23.3 Syntax Description

group-name	DHCP server group name.

1.23.4 Default

DHCP servers are assigned to the default DHCP server group.

1.23.5 Usage Guidelines

Use the **server-group** command to assign a DHCP server to a DHCP server group.

Use the **no** form of this command to assign a DHCP server to the default server group.

1.23.6 Examples

The following example shows how to assign DHCP server, **dserver7**, to the **int-grp** DHCP server group:

```
[local]Redback(config-ctx)#dhcp relay server dserver7

[local]Redback(config-dhcp-relay)#server-group int-grp

[local]Redback(config-dhcp-relay)#
```

1.24 server-mode (NTP)

server-mode

{**no** | **default**} **server-mode**

1.24.1 Purpose

Enables NTP server functionality in the context.

1.24.2 Command Mode

NTP server configuration

1.24.3 Syntax Description

This command has no keywords or arguments.

1.24.4 Default

NTP functionality is not enabled in the context.

1.24.5 Usage Guidelines

To enable NTP server functionality in a context, enter the **server-mode** command in NTP server configuration mode.

1.24.6 Examples

The following example shows how to enable NTP server functionality in the isp202 context.

```
[local]Redback(config)#context isp202
[local]Redback(config-ctx)#ntp-mode
[local]Redback(config-ntp-server)#server-mode
```

1.25 service

service *protocol* [**client**] [**server**]

no service *protocol* [**client**] [**server**]

1.25.1 Purpose

Enables application-layer protocols in a context.

1.25.2 Command Mode

Context configuration

1.25.3 Syntax Description

protocol	Type of service to enable, according to one of the following keywords: • **ftp**—Specifies the File Transfer Protocol (FTP). • **rcp**—Specifies the Remote Copy Protocol (RCP). • **scp**—Specifies the Secured Copy Protocol (SCP). • **sftp**—Specifies the Secured FTP (SFTP). • **ssh**—Specifies Secure Shell (SSH) service. • **telnet**—Specifies Telnet service. • **tftp**—Specifies the Trivial FTP (TFTP).
client	Optional. Enables the protocol's client.
server	Optional. Enables the protocol's server. This keyword is not supported with the FTP and RCP protocols.

1.25.4 Default

The FTP, RCP, SCP, SFTP, SSH, Telnet, and TFTP servers are enabled in the local context and disabled in all other contexts; the SCP, SFTP, SSH, Telnet, and TFTP clients are enabled in all contexts.

1.25.5 Usage Guidelines

Use the **service** command to enable application-layer protocols in a context.

Use the **no** form of this command to disable application-layer protocols in a context.

1.25.6 Examples

The following example shows how to enable Telnet service:

```
[local]Redback(config-ctx)#service telnet
```

1.26 service air-filter

service air-filter

1.26.1 Purpose

Updates the air filter service date for the supported SmartEdge chassis to the current month and year.

1.26.2 Command Mode

Exec

1.26.3 Syntax Description

This command has no keywords or arguments.

1.26.4 Default

The service date is not updated; if the alarm for the air filter is enabled, the alarm condition is raised based on the previous service date.

1.26.5 Usage Guidelines

Use the **service air-filter** command to update the service date for the supported SmartEdge chassis to the current month and year. The service date is stored in the EEPROM in the unit.

Note: The SmartEdge 100 router does not support this command; its air filter is not managed by the SmartEdge OS.

Caution!

Risk of equipment damage. You can corrupt the EEPROM for the fan tray unit or fan and alarm unit in which the service date is stored if you remove the unit from the chassis while the service air-filter command is running. To reduce the risk, do not attempt to remove the unit until after the command is completed.

If you have configured the alarm for the air filter with the **`system alarm`** command in global configuration mode, you must enter this command after you replace the air filter in the supported SmartEdge chassis. Otherwise, the alarm condition is raised based on the previous service date.

To display the current service date, enter the **`show hardware fantray detail`** command in any mode.

1.26.6 Examples

The following example shows how to update the service date with the current month and year. If the current date is February 2005, and the alarm has been enabled with a three-month service interval, the alarm condition becomes active in May 2005:

```
[local]Redback#service air-filter
```

1.27 service auto-system-recovery

`service auto-system-recovery`

`no service auto-system-recovery`

1.27.1 Purpose

Enables automatic system recovery.

1.27.2 Command Mode

Global configuration

1.27.3 Syntax Description

This command has no keywords or arguments.

1.27.4 Default

Automatic system recovery is disabled.

1.27.5 Usage Guidelines

Use the **service auto-system-recovery** command to enable automatic system recovery.

Automatic system recovery allows the system to recover from an error condition in which a process halts. The recovery is carried out by switching to the standby controller card while reloading the current controller card. If the standby controller is not ready or is absent, only a reload is performed.

Note: The SmartEdge 100 router does not have a standby controller card.

Use the **no** form of this command to disable automatic system recovery.

1.27.6 Examples

The following example shows how to enable automatic system recovery:

```
[local]Redback(config)#service auto-system-recovery
```

1.28 service card-auto-reload

service card-auto-reload

no service card-auto-reload

1.28.1 Purpose

Enables the automatic reload of the Packet Processing ASIC (PPA) code on a traffic card if either of its PPAs becomes inoperable.

1.28.2 Command Mode

Global configuration

1.28.3 Syntax Description

This command has no keywords or arguments.

1.28.4 Default

The PPA code reloads automatically on a traffic card if either of the PPAs becomes inoperable.

1.28.5 Usage Guidelines

Use the **`service card-auto-reload`** command to automatically reload the PPA code on a traffic card if either of its PPAs becomes inoperable.

Use the **`no`** form of this command to disable the automatic reload of PPA code on a traffic card.

Note: You enter this command only once to enable automatic reload of the PPA code for any traffic card.

1.28.6 Examples

The following example shows how to configure the system to automatically reload PPA code on a traffic card on a traffic card if either of its PPAs becomes inoperable:

```
[local]Redback(config)#service card-auto-reload
```

1.29 service clips dhcp

```
service clips dhcp [allow-duplicate-mac | source-mac]
[ignore-relay] [maximum max-num] [context ctx-name |
{vendor-class-id [default default-id]}] [service-policy
pol-name]

no service clips
```

1.29.1 Purpose

Enables dynamic clientless IP service selection (CLIPS) on an Ethernet port, 802.1Q permanent virtual circuit (PVC) on an Ethernet port, 802.1Q on-demand PVC , dot1q static PVC, or Asynchronous Transfer Mode (ATM) PVC.

1.29.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Link group configuration
- Link group PVC configuration
- Port configuration

1.29.3 Syntax Description

`allow-duplicate-mac`	Optional. Allows duplicate MAC addresses on dynamic CLIPS circuits; the default state does not allow duplicate MAC addresses. Rather than determining subscriber session uniqueness based on a MAC address alone and rejecting such DHCP request messages, the SmartEdge router uses a combination of the MAC address and the DHCP relay agent IP address to uniquely identify CLIPS clients. In this case, the `giaddr` field in the DHCP request message must be unique.
`service-policy` ***`pol-name`***	Optional. Name of the service policy to which the CLIPS circuits on this PVC must conform. This construct provides access control to the SmartEdge router based on DHCP option 12 (hostname). The policy definition uses **`allow`** and **`deny`** commands in service policy configuration mode to establish a list of hostnames that are allowed access to the SmartEdge router and a list of hostnames that are denied access. For more information about service policies, see *Configuring Service Policies*.
`ignore-relay`	Optional. Allows the SmartEdge OS to ignore the DHCP `giaddr` option and treats the CLIPS subscribers as if they are directly connected to the SmartEdge OS. Use the **`ignore-relay`** keyword to allow the SmartEdge OS to ignore the DHCP `giaddr` option and treat CLIPS subscribers as if they are directly connected to the SmartEdge OS. This keyword is typically used when the CLIPS subscribers are connected to the SmartEdge OS by a Layer 2 switch, which acts as an IP-aware DHCP Relay.
`maximum` ***`max-num`***	Optional. Maximum number of CLIPS sessions allowed on this circuit. The range of values is 1 to 16,000; the default value is 16,000.
`context` ***`ctx-name`***	Optional. Name of the context in which the subscriber is authenticated.

source-mac	Optional. Associates incoming data packets with a parent CLIPS circuit, based on the source MAC address; that is, the SmartEdge system uses the source MAC address to demultiplex the incoming packet traffic per subscriber. The default (when **source-mac** is not specified) sorts incoming packets based only on the source IP addresses.
vendor-class-id [default ***default-id***	Uses the vendor-class-identifier from DHCP packets for selection of the context in which subscribers are authenticated. The DHCP option-60 attribute is the vendor-class-identifier. The received vendor-class-identifier can have a maximum of 48 characters. Use **default** ***default-id*** to specify a default vendor-class-identifier with a maximum of 48 characters.

1.29.4 Default

CLIPS is disabled.

1.29.5 Usage Guidelines

Use the **service clips dhcp** command to enable dynamic CLIPS on an Ethernet port, 802.1Q PVC on an Ethernet port or a link group , or ATM PVC.

The following are the guidelines for this command.

- You can enable CLIPS service on this circuit using the **service clips dhcp** command, or you can assign this circuit to a CLIPS group, using the **service clips-group** command in dot1q PVC or port configuration mode, but you cannot do both.

- giaddr guidelines

  You can specify a unique IP address for the `giaddr` field using the **user-class-id** or **vendor-class-id** command in DHCP giaddr configuration mode; if you do not, the SmartEdge OS uses the primary IP address of the interface that you have configured for the DHCP server for the `giaddr` field.

- Authentication context guidelines

  – To use the **context** ***ctx-name*** construct or the **vendor-class-id** keyword, you must configure the IP address of a reachable RADIUS server and enable subscriber authentication in the context in which the subscriber circuit is to be bound. Use the **radius server** and **aaa**

  authentication subscriber commands in context configuration mode, respectively.

  - The format of the username sent in access-request and accounting packets to RADIUS is MAC-address@domain, where the domain name is the authentication context.

  - If the subscriber record is stored on a RADIUS server and you do not enter either the **context** ***ctx-name*** construct or the **vendor-class-id** keyword, the system authenticates the subscriber in the context defined with the **aaa last-resort** command in context configuration mode.

- Dynamic CLIPS on 802.1Q PVC

  You can configure a QoS policy on the parent CCOD circuit, which gets inherited to the subscriber or by applying the QoS policy directly under the subscriber record by using CLI or RADIUS.

  Here are the guidelines for QoS support for dot1q on-demand circuits:

  - You can configure QoS policing and metering policies at the parent CCOD circuit by using the **inherit** or **hierarchical** keyword, which results in the subscriber getting a QoS policy.

  - The **inherit** keyword results in a subscriber circuit provision with the parent QoS policy if the subscriber circuit does not have a policy of its own.

  - The **hierarchical** keyword results in the CLIPS subscriber circuit being provisioned to the parent QoS policing and metering policy in addition to its own policy if it has any.

  - A QoS queuing policy configured on the parent CCOD circuit is inherited by the CLIPS subscriber circuit if it does not have its own queuing policy.

  - A QoS queuing policy configured under the subscriber record results in all the subscriber traffic using the queues configured in the direct queuing policy.

  - Features like propagate Qos to and from, overhead profile have the same syntax as applicable PPPoE subscriber circuits.

  - The **qos priority** and **rate-circuit** commands, which are supported on static PVCs, are not supported on CCOD circuits.

Note: When a new QoS policy binding configuration under the on demand dot1q pvc or range is applied, the configuration is applied only to new CCOD circuits and subscribers coming up. There is no impact to existing CCOD circuits and subscribers.

When you remove the QoS configuration from the dot1 on-demand PVC configuration, there is no impact to existing CCOD circuits and CLIPS subscriber circuits. New CCOD circuits or CLIPS subscriber circuits coming up will use the existing QoS bindings on the parent CCOD circuit.

The following access control list (ACL) features are supported:

- IPv4 ACL IP Filtering - applied to subscriber
- IPv4 ACL Policy Filtering - Used by QoS
- IPv4 ACL Policy Filtering - Used by Forwarding policy on subscriber
- IPv4 ACL Policy Filtering - Used by NAT policy on subscriber

The following are not supported:

- CLIPS over ATM on-demand PVCs
- CCOD for both CLIPS SVLAN and CVLAN at the same time.
- Netop for configuring CLIPS over on-demand dot1q PVCs.
- Bind interface configuration for dot1q on-demand PVCs
- The range over on-demand dot1q PVCs is not displayed in the **`show configuration port`** command.
- CLIPS support on CCOD is not provided when the **`aaa context`** ***`ctx-name`*** and its attributes are enabled on the dot1q on-demand PVC. The **`aaa context`** ***`ctx-name`*** is used as an alternative mechanism of retrieving the encapsulation type, username, context and other binding attributes from RADIUS, instead of using the configuration.

The following are not supported on CCOD circuits:

- qos priority
- rate-circuit
- circuit-group-member
- forward policy
- forward output
- service clips-exclude

– service clips-group

The following table illustrates the change of CLIPS behavior when the configuration is changed from the initial configuration to the final configuration when both regular and dynamic CLIPS on dot1q on-demand PVC configuration exists on the same PVC.

Table 17 Behavior of CLIPS When Both Regular and On-demand Configuration for the Same PVC Exists

Case	Result of Initial Configuration	Result of Final Configuration	Expected Behavior

1	`port ethernet 2/1`
	` no shutdown`
	` encapsulation dot1q`
	` dot1q pvc on-demand 1`
	`    service clips ...`
		`port ethernet 2/1`
		` no shutdown`
		` encapsulation dot1q`
		` dot1q pvc on-demand 1`
		`    service clips ...`
		` dot1q pvc 1`
		`    service clips ...`
			CLIPS subscriber sessions (if any) on “on-demand pvc 1” session are torn down. Recovery can occur over “pvc 1” depending on configuration and lease times.
			Packets are dropped during the transition from on-demand configuration of the session to static configuration.

2	`port ethernet 2/1`
	` no shutdown`
	` encapsulation dot1q`
	` dot1q pvc 1`
	`    service clips ...`
		`port ethernet 2/1`
		` no shutdown`
		` encapsulation dot1q`
		` dot1q pvc on-demand 1`
		`    service clips ...`
		` dot1q pvc 1`
		`    service clips ...`
			No impact on CLIPS subscribers (if any).

Table 17 Behavior of CLIPS When Both Regular and On-demand Configuration for the Same PVC Exists

Case	Result of Initial Configuration	Result of Final Configuration	Expected Behavior

3	`port ethernet 2/1`
	` no shutdown`
	` encapsulation dot1q`
	` dot1q pvc on-demand 1`
	`    service clips ...`
	` dot1q pvc 1`
	`    service clips`
		`port ethernet 2/1`
		` no shutdown`
		` encapsulation dot1q`
		` dot1q pvc on-demand 1`
		`    service clips ...`
			CLIPS subscribers (if any) on “pvc 1” session are torn down. Recovery can occur, depending on the configuration, lease times and when “on-demand pvc 1” is created based on packet activity.
			Packets are dropped during the transition from static pvc configuration of the session to on-demand circuit configuration.

4	`port ethernet 2/1`
	` no shutdown`
	` encapsulation dot1q`
	` dot1q pvc on-demand 1`
	`    service clips ...`
	` dot1q pvc 1`
	`    service clips ...`
		`port ethernet 2/1`
		` no shutdown`
		` encapsulation dot1q`
		` dot1q pvc 1`
		`    service clips ...`
			No impact on CLIPS subscribers.

Use the `no` form of this command to disable CLIPS service.

For more information about dynamic CLIPS on dot1q on-demand PVC, see *Configuring CLIPS*.

1.29.6 Examples

1.29.6.1 CLIPS Static Circuits

The following example shows how to create eight CLIPS static circuits with session numbers ranging from **1** to **8** on port **1** of the Ethernet traffic card installed in slot **3** and then bind each circuit to an automatically generated subscriber name beginning with the string **10-1-1:**

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#service clips
[local]Redback(config-port)#clips pvc 1 through 8
[local]Redback(config-port)#bind auto-subscriber “10-1-1” local
```

1.29.6.2 Dynamic CLIPS

The following example shows how to enable dynamic CLIPS on port **1** of the Ethernet traffic card installed in slot **3**, using the **pol-dhcp** service policy:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#service clips dhcp service-policy pol-dhcp
```

1.29.6.3 CLIPS subscribers to act as if they are directly connected to the SmartEdge OS

The following example shows how to allow the CLIPS subscribers to act as if they are directly connected to the SmartEdge OS on port **1** on the Ethernet traffic card installed in slot **1:**

```
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 10
[local]Redback(config-dot1q-pvc)#service clips dhcp ignore-relay context dhcp
```

1.29.6.4 CLIPS Subscribers on the Ethernet traffic card

The following example shows how to allow the CLIPS subscribers that use port **2** on the Ethernet traffic card installed in slot **1** to have duplicate MAC addresses; the unique giaddr is specified using the secondary IP address assigned to the **if-dhcp** interface:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface if-dhcp multibind
[local]Redback(config-if)#ip address 200.1.1.1/24
[local]Redback(config-if)#ip address 200.1.2.1/24 secondary
[local]Redback(config-if)#dhcp proxy 16000
[local]Redback(config-dhcp-giaddr)#user-class-id net1 giaddr 200.1.2.1
[local]Redback(config-dhcp-giaddr)#end
[local]Redback(config)#port ethernet 1/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 10
[local]Redback(config-dot1q-pvc)#service clips dhcp allow-duplicate-mac
```

1.29.6.5 Dynamic CLIPS on 802.1Q On-Demand PVC

The following example shows how to configure a dynamic CLIPS on dot1q On-Demand PVC.

```
[local]Redback(config-port)#dot1q pvc on-demand 1 through 2
[local]Redback(config-dot1q-pvc)#service clips dhcp
[local]Redback(config-dot1q-pvc)#end
```

Regular and on-demand PVCs with the same dot1q PVC id are supported. However, regular dot1q PVC configuration takes precedence over on-demand PVC configuration. For example:

```
[local]Redback(config-port)#dot1q pvc on-demand 1
[local]Redback(config-port)#dot1q pvc 1

[local]Redback#show configuration port 2/1
!
port ethernet 2/1
 no shutdown
 encapsulation dot1q
 dot1q pvc on-demand 1
 dot1q pvc 1          <= Overrides the on-demand configuration
```

1.30 service clips-exclude user-class-id

service clips-exclude user-class-id *id* [**offset** *position*]

{**no** | **default**} **service clips-exclude user-class-id** *id* [**offset** *position*]

1.30.1 Purpose

Specifies a condition by which a Dynamic Host Configuration Protocol (DHCP) host can be excluded from clientless IP service selection (CLIPS) service on this port or permanent virtual circuit (PVC).

1.30.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Link group configuration
- Link PVC configuration
- Port configuration

1.30.3 Syntax Description

`user-class-id` *`id`*	Contents of the DHCP option-77 ID field that is to be excluded, in one of the following formats: • Alphanumeric string, enclosed in quotation marks (“ ”); for example, “ABCD1234” • Alphanumeric string, not enclosed in quotation marks; for example, corp123 • Hex numeric string, not enclosed in quotation marks and prefaced with 0x or 0X; for example, 0Xabcd1234 There is no default value.
`offset` *`position`*	Optional. Position of the starting octet to which the exclusion condition is to be matched, according to one of the following formats: • `+`*`n`* or *`n`*—Starting octet is the *`n`*th octet in the received ID. The matching operation is performed on the *`n`*th and succeeding octets for the length of the string specified by the `user-class-id` *`id`* construct. • `-`*`n`*—Starting octet is the last octet in the received ID minus the previous (*`n`*-1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the `user-class-id` *`id`* construct. The range of values is -254 to 254. If offset is not configured, the starting octet is 1.

1.30.4 Default

No DHCP hosts are excluded from CLIPS service.

1.30.5 Usage Guidelines

Use the **`service clips-exclude user-class-id`** command to specify a user-class condition by which a DHCP host can be excluded from CLIPS service on this port or PVC. Any host that matches the exclusion condition is ineligible for CLIPS service and is treated as a normal DHCP client.

The **service clips-exclude user-class-id** command works in conjunction with the **service clips-exclude vendor-class-id** command, which uses DHCP option 60. If the SmartEdge router is configured for CLIPS exclusion based on both DHCP option 60 and option 77, then:

- If either option matches, the host is excluded from CLIPS service.
- If neither option matches, a CLIPS session is set up for the host.

Note: You must first enable dynamic CLIPS service for this port or PVC using the **service clips** or **service clips-group** command in ATM PVC, dot1q PVC, link group, link PVC, or port configuration mode. You must also configure an external proxy or internal DHCP server in the same context as that in which the host messages are received.

The following guidelines apply to the formats for the *id* argument:

- When you surround a string with quotation marks, they are not part of the comparison.
- You must enclose a string with quotation marks if the string includes a space.
- A hex numeric string must have an even number of characters.
- Any string format, alphanumeric or hex numeric, supports both uppercase and lowercase characters.

Matching is performed on a per-octet basis. The match fails if after the calculation of the starting position of the octets to be matched (using the **offset** ***position*** construct), there are fewer octets available for matching in the received ID than are specified by the **user-class-id** ***id*** construct.

To specify multiple exclusion conditions, enter this command for each condition; a DHCP host is excluded if it matches any of the specified conditions.

Use the **no** or **default** form of this command to remove an exclusion condition from the configuration for this port or PVC.

1.30.6 Examples

The following example shows how to configure an Ethernet port for CLIPS service and excludes DHCP hosts with a user class of **"user-class1"** and an offset of **3** octets. The matching operation is performed on the 3rd through the 13th octet. If the received ID is user-class1, the matching operation is successful.

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#service clips-exclude user-class-id user-class1 offset 3
```

1.31 service clips-exclude vendor-class-id

`service clips-exclude vendor-class-id` *`id`* [**`offset`** *`position`*]

{**`no`** | **`default`**} **`service clips-exclude vendor-class-id`** *`id`* [**`offset`** *`position`*]

1.31.1 Purpose

Specifies a condition by which a Dynamic Host Configuration Protocol (DHCP) host can be excluded from clientless IP service selection (CLIPS) service on this port or permanent virtual circuit (PVC).

1.31.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Link group configuration
- Link PVC configuration
- Port configuration

1.31.3 Syntax Description

`vendor-class-id` *`id`*	Contents of the DHCP option-60 ID field that is to be excluded, in one of the following formats: • Alphanumeric string, enclosed in quotation marks (“ ”); for example, “ABCD1234” • Alphanumeric string, not enclosed in quotation marks; for example, corp123 • Hex numeric string, not enclosed in quotation marks and prefaced with 0x or 0X; for example, 0Xabcd1234
`offset` *`position`*	Optional. Position of the starting octet to which the exclusion condition is to be matched, according to one of the following formats: • *+n* or *n*—Starting octet is the *n*th octet in the received ID. The matching operation is performed on the *n*th and succeeding octets for the length of the string specified by the **`vendor-class-id`** *`id`* construct. • *-n*—Starting octet is the last octet in the received ID minus the previous (*n*-1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the **`vendor-class-id`** *`id`* construct. The default value is 1 (the first octet).

1.31.4 Default

No DHCP hosts are excluded from CLIPS service.

1.31.5 Usage Guidelines

Use the **`service clips-exclude vendor-class-id`** command to specify a condition by which a DHCP host can be excluded from CLIPS service on this port or PVC. Any host that matches the exclusion condition is ineligible for CLIPS service and is treated as a normal DHCP client.

The **`service clips-exclude vendor-class-id`** command works in conjunction with the **`service clips-exclude user-class-id`** command, which uses DHCP option 77. If the SmartEdge router is configured for CLIPS exclusion based on both DHCP option 60 and option 77, then:

- If either option matches, the host is excluded from CLIPS service.
- If neither option matches, a CLIPS session is set up for the host.

Note: You must first enable dynamic CLIPS service for this port or PVC using the **`service clips`** or **`service clips-group`** command in ATM PVC, dot1q PVC, link group, link PVC, or port configuration mode. You must also configure an external proxy or internal DHCP server in the same context as that in which the host messages are received.

The following guidelines apply to the formats for the *`id`* argument:

- When you surround a string with quotation marks, they are not part of the comparison.

- You must enclose a string with quotation marks if the string includes a space.

- A hex numeric string must have an even number of characters.

- Any string format, alphanumeric or hex numeric, supports both uppercase and lowercase characters.

Matching is performed on an octet basis. The match fails if after the calculation of the starting position of the octets to be matched (using the **`offset`** *`position`* construct), there are fewer octets available for matching in the received ID than are specified by the **`vendor-class-id`** *`id`* construct.

To specify multiple exclusion conditions, enter this command for each condition; a DHCP host is excluded if it matches any of the specified conditions.

Use the **`no`** or **`default`** form of this command to remove an exclusion condition from the configuration for this port or PVC.

1.31.6 Examples

The following example shows how to configure an Ethernet port for CLIPS service and excludes DHCP hosts with an ID of **"BP29"** and an offset of **3** octets. The matching operation is performed on the 3rd through the 6th octet. If the received ID is CCBP2945, the matching operation is successful:

```
[local]Redback(config)#port ethernet 14/1
[local]Redback(config-port)#service clips-exclude vendor-class-id "BP29" offset 3
```

In the following example, the same matching operation is performed but with an offset of –3. In this case, the matching operation starts at the 6th octet and the match always fails because the number of octets to be matched (4) is greater than the number of octets available to be matched.

```
[local]Redback(config)#port ethernet 14/1
[local]Redback(config-port)#service clips-exclude vendor-class-id "BP29" offset -3
```

1.32 service clips-group

`service clips-group` ***`group-name`***

`no service clips-group` ***`group-name`***

1.32.1 Purpose

Assigns a port or permanent virtual circuit (PVC) to the specified clientless IP service selection (CLIPS) group.

1.32.2 Command Mode

- dot1q PVC configuration
- Port configuration

1.32.3 Syntax Description

`group-name`	Name for a CLIPS group of ports and PVCs on which dynamic CLIPS circuits will be created.

1.32.4 Default

No ports or PVCs are assigned to any CLIPS group.

1.32.5 Usage Guidelines

Use the **`service clips-group`** command to assign this port or PVC to the specified CLIPS group. You can assign any mix of ports and PVCs to a CLIPS group. When you assign the port or PVC to the CLIPS group, you enable the creation dynamic CLIPS service on that port or PVC.

You must first create the CLIPS group, using the **`clips-group`** command in global configuration mode, before you can assign a port or PVC to it.

You cannot assign ports and PVCs that you have configured on different traffic cards to the same CLIPS group; that is, CLIPS group supports intra-card, inter-port redundancy, but not inter-card redundancy.

You can enable dynamic CLIPS service on this circuit using the **`service clips dhcp`** command in ATM PVC, dot1q PVC, or port configuration mode, or you can assign this port or PVC to a CLIPS group, but you cannot do both.

Use the **`no`** form of this command to remove the port or PVC from the specified CLIPS group.

Note: This command is available only for Ethernet and Gigabit Ethernet ports and the 802.1Q PVCs configured on them.

1.32.6 Examples

The following example shows how to assign an 802.1Q PVC on an Ethernet port to the **dynamic-clips** group:

```
[local]Redback(config)#port ethernet 4/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 3
[local]Redback(config-dot1q-pvc)#service clips-group dynamic-clips
```

1.33 service clips (static)

```
service clips
```

```
no service clips
```

1.33.1 Purpose

Enables static clientless IP service selection (CLIPS) on an Ethernet port, 802.1Q permanent virtual circuit (PVC) on an Ethernet port, or Asynchronous Transfer Mode (ATM) PVC.

1.33.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Link group configuration
- Link PVC configuration
- port configuration

1.33.3 Syntax Description

This command has no keywords or arguments.

1.33.4 Default

CLIPS is disabled.

1.33.5 Usage Guidelines

Use the **service clips** command to enable static CLIPS on an Ethernet port, 802.1Q PVC on an Ethernet port, or ATM PVC.

For static CLIPS circuits, you must also configure one or more CLIPS PVCs using the **clips pvc** command (in link group, link PVC, or port configuration mode; see the **clips pvc** command description.

You can enable CLIPS service on this circuit using the **service clips** command, or you can assign this circuit to a CLIPS group, using the **service clips-group** command in dot1q PVC or port configuration mode, but you cannot do both.

Use the **no** form of this command to disable CLIPS service.

1.33.6 Examples

The following example shows how to create eight CLIPS static circuits with session numbers ranging from **1** to **8** on port **1** of the Ethernet traffic card installed in slot **3** and then bind each circuit to an automatically generated subscriber name beginning with the string **10-1-1:**

```
[local]Redback(config)#port ethernet 3/1

[local]Redback(config-port)#service clips

[local]Redback(config-port)#clips pvc 1 through 8

[local]Redback(config-port)#bind auto-subscriber “10-1-1” local
```

1.34 service console-break

service console-break

no service console-break

1.34.1 Purpose

Enables the console break feature.

1.34.2 Command Mode

Global configuration

1.34.3 Syntax Description

This command has no keywords or arguments.

1.34.4 Default

The console break feature is disabled.

1.34.5 Usage Guidelines

Use the **service console-break** command to enable the console break feature. When this feature is enabled, you can press the **Ctrl+Break** keys in sequence when you are connected to the SmartEdge router through the console port to send a break sequence to the system to halt the system, and enter kernel debug mode.

After the system receives the break sequence from the console, the prompt changes to **db>**. At this point, you can enter the commands in Table 18.

Table 18 Kernel Debug Mode Commands

Kernel Debug Command	**Description**
continue	Resumes normal system operation.
reboot	Reloads the system (has the same effect as the **reload** command in exec mode).

The system waits for a command for 25 seconds. If you do not enter any command within this time, the system automatically reloads.

Caution!

Risk of data loss. If the console port is directly attached to the serial port of a computer running Windows NT or UNIX, the computer might send a break sequence when it reboots. This has the affect of halting the system and entering kernel debug mode. To reduce the risk, do not enable the console-break feature if the workstation attached to the console port is running Windows NT or UNIX.

Use the **no** form of this command to disable the console break feature. When the feature is disabled, the system does not process a break sequence from the console port.

1.34.6 Examples

The following example shows how to enable the console break feature:

```
[local]Redback(config)#service console-break
```

1.35 service crash-dump-dram

`service crash-dump-dram`

`no service crash-dump-dram`

1.35.1 Purpose

Enables dynamic random-access memory (DRAM) data collection during a crash dump.

1.35.2 Command Mode

Global configuration

1.35.3 Syntax Description

This command has no keywords or arguments.

1.35.4 Default

DRAM data collection is enabled.

1.35.5 Usage Guidelines

Use the **`service crash-dump-dram`** command to enable DRAM data collection during a crash dump.

Use the **`no`** form of this command to disable DRAM data collection during a core dump. In situations where the Packet Processing ASIC (PPA) data collection might take a long time, you can use the **`no`** form of this command to skip the DRAM data collection.

Note: The **`reload card`** command in exec mode suppresses the in-progress DRAM data collection if confirmed by user.

Note: Because DRAM data collection during a crash dump is enabled by default, the **`service crash-dump-dram`** command is used only to return the router to its default behavior after it has been changed by the **`no`** form of this command.

1.35.6 Examples

The following example shows how to disable the DRAM data collection during a crash dump:

```
[local]Redback(config)#no service crash-dump-dram
```

1.36 service domain-wildcard

service domain-wildcard

no service domain-wildcard

1.36.1 Purpose

Enables the creation of domain aliases with embedded wildcard characters.

1.36.2 Command Mode

Global configuration

1.36.3 Syntax Description

This command has no keywords or arguments.

1.36.4 Default

Wildcards are not permitted in domain name aliases.

1.36.5 Usage Guidelines

Use the **service domain-wildcard** command in global configuration mode to enable the creation of domain aliases with embedded wildcard characters. See the **domain** command for rules on the use of domain name alias wildcard characters.

Use the **no** form of this command to disable the use of the * wildcard character.

1.36.6 Examples

The following example illustrates the creation of the **ERIC*** and ***com** domain aliases for the context **bar3** and the **ER*** and **bob*bar3** domain aliases for the context **bob:**

```
[local]Redback(config)#service domain-wildcard
[local]Redback(config)#context bar3
[local]Redback(config-ctx)#domain ERIC*
[local]Redback(config-ctx)#domain *com
[local]Redback(config-ctx)#commit
[local]Redback(config-ctx)#exit
[local]Redback(config)#context bob
[local]Redback(config-ctx)#domain ER*
[local]Redback(config-ctx)#domain bob*bar3
[local]Redback(config-ctx)#commit
```

1.37 service inter-context routing

```
service inter-context routing
no service inter-context routing
```

1.37.1 Purpose

Enables intercontext static routing among non-local contexts.

1.37.2 Command Mode

Global configuration

1.37.3 Syntax Description

This command has no keywords or arguments.

1.37.4 Default

Disabled

1.37.5 Usage Guidelines

Use the **`service inter-context routing`** command to enable intercontext static routing among non-local contexts. When this command is not enabled, intercontext static routing can still be used between the local context and non-local contexts.

Intercontext routing enables the creation of routing sessions between peers that belong to different contexts that are not connected by a physical port, eliminating the need fo an actual physical link between the contexts.

Note: This command can only be disabled when there is no instance of non-local context static routing configured on the router.

For more information on creating and servicing contexts, see *Configuring Contexts and Interfaces*.

1.37.6 Examples

The following example enables non-local inter-context static routing:

```
[local]Redback(config)#service inter-context routing

[local]Redback(config)#context cust-abc

[local]Redback(config-ctx)#ip route 11.1.1.0/24 context web-xyz

[local]Redback(config-ctx)#context web-xyz

[local]Redback(config-ctx)#ip route 12.2.0.0/16 context cust-abc
```

1.38 service load-balance ip

`service load-balance ip {layer-3 | layer-4}`

1.38.1 Purpose

Specifies whether the load balancing hash algorithm should include only Layer 3 information or both Layer 3 and Layer 4 information.

1.38.2 Command Mode

Global configuration

1.38.3 Syntax Description

`layer-3`	Specifies that the load balancing algorithm includes Layer 3 information only; that is, source and destination IP only.
`layer-4`	Specifies that the load balancing algorithm includes both Layer 3 and Layer 4 information, that is, source and destination IP and source and destination ports for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets.

1.38.4 Default

The load balancing algorithm includes Layer 3 information only.

1.38.5 Usage Guidelines

Use the **`service load-balance ip`** command to specify whether the load balancing hash algorithm should include only Layer 3 information or both Layer 3 and Layer 4 information. Layer 3 information consists of the source and destination IP. Layer 4 information includes the destination ports for TCP and UDP packets.

Including the TCP and UDP source and destination ports in the load balancing hash algorithm provides the following functionality:

- Balancing the traffic load among available paths while keeping packets for a particular data flow in order.

- Preserving the same path for all packets in a given flow.

Note: The **`service load-balance ip`** command is supported only on IPV4 and only for complete packets. It is not supported for IPv6 or when IP fragmentation is used.

Note: Use the **`show ip route summary`** command to verify whether Layer 4 load balancing is enabled on a router.

1.38.6 Examples

The following example shows how to configure the load balancing algorithm to include both Layer 3 and Layer 4 information:

```
[local]Redback#configure

[local]Redback(config)#service load-balance ip layer-4
```

The following example shows how to return the load balancing algorithm to the default setting, which includes only Layer 3 information:

```
[local]Redback#configure

[local]Redback(config)#service load-balance layer-3
```

1.39 service multiple-contexts

`service multiple-contexts`

`no service multiple-contexts`

1.39.1 Purpose

Enables the creation of multiple contexts on a system.

1.39.2 Command Mode

Global configuration

1.39.3 Syntax Description

This command has no keywords or arguments.

1.39.4 Default

Multiple contexts are disabled.

1.39.5 Usage Guidelines

Use the **`service multiple-contexts`** command to enable the creation of multiple contexts on a system. By default, the “local” context is present, and you cannot use the **`context`** command in global configuration mode to create additional contexts until you enable the multiple context feature.

Use the **`no`** form of this command to disable multiple contexts.

1.39.6 Examples

The following example displays sample output when an administrator attempts to create a new context, **netone**, and the multiple context feature is disabled:

```
[local]Redback(config)#context netone
```

```
Context netone doesn't exist.

To configure multiple contexts configure 'service multiple-contexts'
```

The following example shows how to enable the multiple context feature and creates the context, **netone:**

```
[local]Redback(config)#service multiple-contexts

[local]Redback(config)#context netone
```

1.40 service-policy

service-policy name *svc-pol-name*

no service-policy name *svc-pol-name*

1.40.1 Purpose

Configures a service policy name and enters service policy configuration mode.

1.40.2 Command Mode

Global configuration

1.40.3 Syntax Description

name *svc-pol-name*	Service policy name.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **service-policy** command to configure a service policy name and enter service policy configuration mode.

Use the **no** form of this command to remove a service policy.

1.40.6 Examples

The following example shows how to configure a service policy, **local-only**, and allow subscribers access to the **local** context only:

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#allow context name local
```

1.41 service profile hotline

service profile hotline*profile-name*

no service profile hotline *profile-name*

1.41.1 Purpose

Specifies an RSE profile that references a policy that defines the classes to which you want to map HTTP redirect rules.

1.41.2 Command Mode

Subscriber configuration

1.41.3 Syntax Description

profile-name	Name of an RSE profile that references a policy that defines the classes to which HTTP redirect rules will be mapped.

1.41.4 Default

No RSE profile is specified for hotlining.

1.41.5 Usage Guidelines

Use the **service profile hotline** command to specify an RSE profile that references a policy that defines the classes to which you want to map HTTP redirect rules. This command maps the HTTP redirect rules to classes defined in the policy that is referenced in the specified RSE profile for a MIP FA subscriber.

Use the **no** form of this command in to remove the specified service profile so that HTTP redirect rules are not mapped to that classes defined in the referenced policy.

1.41.6 Examples

The following example shows how to specify an RSE profile for hotlining:

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

[local]Redback(config-ctx)#subscriber default

[local]Redback(config-sub)#service profile hotline hp1
```

1.42 service upload-coredump

service upload-coredump ftp:*url* [**context *ctx-name***]

no service upload-coredump

1.42.1 Purpose

Enables sending core dump files from the local SmartEdge router to the specified URL using File Transfer Protocol (FTP).

1.42.2 Command Mode

Global configuration

1.42.3 Syntax Description

ftp: *url*	URL of the server that the system is to send a core dump file using FTP.
context *ctx-name*	Optional. Context for server reachability.

1.42.4 Default

None

1.42.5 Usage Guidelines

Use the **service upload-coredump** command to enable sending core dump files from the local SmartEdge router to a URL using FTP. The ***url*** argument takes the following form, where the ***username*:*passwd*** construct specifies the user and an optional password, the ***ip-addr*** argument is the IP address of the FTP server, the ***hostname*** argument is the hostname of the FTP server, and the optional **:*port*** and **/*directory*** arguments are a port or directory on the FTP server.

//*username*[:*passwd*]@{*ip-addr* | *hostname*} [:*port*] [//*directory*]

The ***hostname*** argument can only be used if Domain Name System (DNS) resolution is enabled using the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode. For more information, see *Command List*.

Note: Use double slashes (//) if the pathname to the directory on the remote server is an absolute pathname; use a single slash (/) if it is a relative pathname (under the hierarchy of the username account home directory).

Note: We strongly recommend that you enable this feature because it maximizes the use of available disk space and improves system stability and performance. For more information about core dumps, crash files, and the operations commands to administer them, see *Managing Files*.

Use the **no** form of this command to disable sending crash files to the specified URL.

1.42.6 Examples

The following example shows how to specify that crash files are sent to the specified URL using FTP:

```
[local]Redback(config)#service upload-coredump ftp://client1:secret@10.10.20.78//out
```

1.43 service vxworks-log-to-screen

service vxworks-log-to-screen

no service vxworks-log-to-screen

1.43.1 Purpose

Enables displaying VxWorks logs on a console connected to one of the console ports on the back of the chassis.

1.43.2 Command Mode

Global configuration

1.43.3 Syntax Description

This command has no keywords or arguments.

1.43.4 Default

By default, the VxWorks console port output is redirected, so it is not displayed even though the console cable is connected.

1.43.5 Usage Guidelines

Use the **`service vxworks-log-to-screen`** command to enable the VxWorks logs to display on a console connected to one of the console ports on the back of the chassis. Use this command to collect logs without interruption during a switchover or when the SmartEdge router is rebooting.

VxWorks is the OS on the controller cards that is responsible for most low-level processing, such as driving or monitoring traffic cards. To display the VxWorks logs on the VxWorks console, you may also need to set the **`vx-other`** flag in the Open Firmware (OFW) shell. To set this flag, access the OFW shell and enter the **`setenv vx-other 0x27a`** command at the `OK` prompt.

For procedures to access the OFW CLI, see *Data Collection Guideline for the SmartEdge Router*.

1.44 session-action

```
session-action {absolute-timeout | dual-stack-failure
force-down | idle-timeout | traffic-limit} account-alive
```

```
no session-action
```

1.44.1 Purpose

Assigns the actions taken when a subscriber reaches a timeout or traffic limit.

1.44.2 Command Mode

Subscriber configuration

1.44.3 Syntax Description

`absolute-timeout`	Clears the subscriber session if it reaches the absolute-timeout limit.
`dual-stack-failure force-down`	Clears the subscriber session if any IPv4 address or IPv6 prefix conflicts are detected.
`idle-timeout`	Clears the subscriber session if it reaches the idle-timeout limit.
`traffic-limit`	Clears the subscriber session if it reaches the traffic limit.
`account-alive`	Sends a RADIUS Account-Alive message.

1.44.4 Default

No action is taken when a subscriber reaches session limits.

1.44.5 Usage Guidelines

Use the **`session-action`** command to assign the actions taken when a subscriber reaches a timeout or traffic limit.

The Account-Alive message contains vendor-specific attribute (VSA) 144 provided by Ericsson AB giving the reason for the session action: volume ingress exceeded, volume egress exceeded, idle timeout, or session timeout (absolute timeout). For more information about vendor VSA 144, see *RADIUS Attributes*.

The specified action is assigned either to a subscriber profile or an individual subscriber record depending on the type of subscriber:

- Default subscriber
- Named subscriber profile
- Named individual subscriber

If an IPv4 address or IPv6 prefix conflict is detected and the **`session-action dual-stack-failure force-down`** command is enabled for a dual-stack subscriber:

- Authentication fails for the affected stack only; the unaffected stack authenticates and the subscriber remains in a state where only one stack is active for the life of the session.
- The SmartEdge router sends an authentication failure message to the AAA client.

- The SmartEdge router sends an Accounting-Stop message to the RADIUS server, as long as Accounting-Stop messages are not suppressed with the `aaa accounting suppress-acct-on-fail` command (without the `except-for-duplicate-ip` keyword).

  Note: If the `aaa accounting suppress-acct-on-fail except-for-duplicate-ip` command is configured, Accounting-Stop messages are still sent.

Use the `no` form of this command to remove the session action from the subscriber record or profile.

1.44.6 Examples

1.44.6.1 Clear the Subscriber Session if it Reaches the Idle-Timeout Limit.

The following example shows how to assign the **idle-timeout account-alive** session action to the subscriber profile named **tomtom:**

```
[local]Redback(config-ctx)#subscriber profile tomtom

[local]Redback(config-sub)#session-action idle-timeout account-alive
```

1.44.6.2 Clear the Subscriber Session if Any IPv4 Address or IPv6 Prefix Conflicts are Detected

The following example shows how to assign the **dual-stack-failure force-down** session action to the subscriber profile named **tomtom:**

```
[local]Redback(config-ctx)#subscriber profile tomtom

[local]Redback(config-sub)#session-action dual-stack-failure force-down
```

1.45 session-action (failure)

```
session-action failure always-up [trap]

no session-action failure always-up
```

1.45.1 Purpose

Enables a subscriber session to be successfully established and remain active, regardless of a misconfigured, nonexistent, or optional subscriber attribute that failed to apply.

1.45.2 Command Mode

Subscriber configuration

1.45.3 Syntax Description

`failure`	Specifies the action to take when subscriber attributes fail to be provisioned.
`always-up`	Keeps the session active regardless of a misconfigured, nonexistent, or optional subscriber attribute that fails to apply.
`trap`	Optional. Enables SNMP traps and logs to be sent to a console to alert administrators, when a subscriber attribute fails to be initially provisioned. The SNMP trap and log includes information about the reason a subscriber attribute failed to be initially provisioned, as well as information about keeping the subscriber session active. To use the keyword **`trap`**, you must have a configured SNMP server.

1.45.4 Default

By default, a subscriber session fails to be established and remain active if a subscriber attribute is misconfigured or nonexistent, or if an optional subscriber attribute fails to be applied.

1.45.5 Usage Guidelines

Use the **`session-action failure always-up`** command to enable a subscriber session to be successfully established and remain active regardless of a misconfigured, nonexistent, or optional subscriber attribute that failed to apply. These subscriber attributes are of the type that can be allowed to be provisioned, regardless of missing subscriber attribute data or a provisioning failure. They can be learned by the SmartEdge OS either through RADIUS or a local subscriber record. The following are examples of these types of subscriber attributes:

- A Filter-id attribute with an access list that is not configured.

- A queueing policy attribute for encapsulation that does not match the actual encapsulation the subscriber uses. For example, the encapsulation type configured on the RADIUS server is ATM PPP over Ethernet (PPPoE), and the actual encapsulation type the subscriber uses is Ethernet PPPoE.

If more than one queuing policy attribute is configured for subscriber encapsulation after the **session-action failure always-up** command is enabled, the SmartEdge OS selects the attribute to apply by matching the queueing policy name and its configured encapsulation type with the actual encapsulation type the subscriber is using. Once matched, the session is established and allowed to remain active.

The **session-action failure always-up** command must be enabled for a subscriber using either the default subscriber profile or a named subscriber profile within the context to which the subscriber is bound.

Use the **trap** keyword to enable the SmartEdge router to send SNMP traps and logs.

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

1.45.6 Examples

The following example shows how to enable the **session-action failure always-up** command for the default subscriber profile within the `local` context, and send SMNP traps and logs about subscriber attributes that failed to apply:

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

[local]Redback(config)#context local

[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#session-action failure always-up trap
```

1.46 session-auth

session-auth {**pap** | **chap** | **chap pap**} [**context** ***ctx-name*** | **service-policy** ***svc-policy-name***]

{**no** | **default**} **session-auth**

1.46.1 Purpose

Specifies the method used by the SmartEdge router when acting as a Layer 2 Tunneling Protocol (L2TP) network server (LNS) to authenticate subscriber sessions that arrive from this peer.

1.46.2 Command Mode

L2TP peer configuration

1.46.3 Syntax Description

`pap`	Specifies that the Password Authentication Protocol (PAP) is to be used to obtain the subscriber name and password from the subscriber.
`chap`	Specifies that the Challenge Handshake Authentication Protocol (CHAP) is to be used to obtain the subscriber name and password from the subscriber.
`chap pap`	Specifies that either PAP or CHAP can be used to obtain the subscriber name and password from the subscriber, but that CHAP is preferred.
context *ctx-name*	Optional. Name of a specific context to which subscriber sessions are restricted.
service-policy *svc-policy-name*	Optional. Name of a service policy that limits the contexts or domains available to the subscriber sessions.

1.46.4 Default

CHAP or PAP is the authentication method.

1.46.5 Usage Guidelines

Use the **session-auth** command to specify the method used by the SmartEdge router when acting as an L2TP LNS to authenticate subscriber sessions that arrive from this peer.

Use this optional command for the following conditions:

- To require specific authentication protocol.
- To limit dynamic service selection to a particular context.
- To specify a service policy.

Use the optional **context** *ctx-name* construct to prevent dynamic context selection, thereby limiting the services available to any Point-to-Point Protocol (PPP) sessions that arrive from this peer. Specifically, these sessions are limited to terminating and routing in the named context and to entering a tunnel defined within that context.

If the **context** *ctx-name* construct is present, the SmartEdge router attempts to authenticate the session according to the authentication, authorization, and accounting (AAA) configuration for the named context, rather than according to the context portion of the structured subscriber name, if present. If the subscriber passes authentication, the session comes up.

If RADIUS returns a Context-Name attribute whose value conflicts with the **context** *ctx-name* construct (or any of its aliases) in the command line, the binding fails. Authentication also fails if global authentication is configured and the Access-Response packet from the RADIUS server does not contain a Context-Name attribute.

Use the optional **service-policy** *svc-policy-name* construct to attach a service policy to the subscriber sessions from this peer. This construct allows you to limit the services to more than one context.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer using the **clear tunnel** command in exec mode, or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** or **default** form of this command to specify the default method to authenticate subscriber sessions.

1.46.6 Examples

The following example shows how to specify that only PAP can be used to authenticate subscriber sessions:

```
[local]Redback(config-ctx)#l2tp-peer name peer1

[local]Redback(config-l2tp)#session-auth pap
```

1.47 session-dampening

session-dampening [*half-life reuse suppress max-suppress-time*]

no session-dampening

1.47.1 Purpose

Enables a flapping peer to be temporarily suppressed for a configurable amount of time.

1.47.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.47.3 Syntax Description

half-life	Optional. Time, in minutes, after which a penalty is decreased. Once the session has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty occurs every 5 seconds. The range of values for the half-life period is 1 to 45; the default value is 15.
reuse	Optional. Value that determines whether a session is unsuppressed and can be reused. When a penalty for a flapping peer decreases to the point that it falls below this value, the session is unsuppressed and can be reused. Sessions are scanned for reuse every 5 seconds. The range of values is 1 to 20,000; the default value is 1,500.
suppress	Optional. Value that determines if a session is suppressed. A session is suppressed when its penalty exceeds this limit. The range of values is 1 to 20,000; the default value is 3,000.
max-suppress-time	Optional. Maximum time in minutes a session can be denied to open. The range of values is 1 to 255; the default value is four times the ***half-life*** argument. If the half-life value is allowed to default, the *maximum-suppress* value defaults to 60.

1.47.4 Default

Session dampening is disabled.

1.47.5 Usage Guidelines

Use the **session-dampening** command to enables a flapping peer to be temporarily suppressed for a configurable amount of time.

This command is per peer and peer-group based. If the peer is member of a peer group, the command is inherited from the peer-group and can be customized in the peer configuration.

The main benefit of this feature is to avoid flapping peers from using system resources, and also to reduce routing churn induced by a flapping peer.

A message is logged when a session is dampened and undampened.

Note: Session dampening is different from route dampening. Session dampening dampens peers when it is reset, and route dampening dampens routes from a peer in established states.

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

1.47.6 Examples

The following example shows how to enable session dampening with a half life of **5** minutes, a reuse value of **1000**, a suppress value of **4000**, and a maximum suppress time of **10** minutes:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#peer-group pi internal
[local]Redback(config-bgp-peer-group)#session-dampening 5 1000 4000 10
```

1.48 session-limit

session-limit {**agent-circuit-id** | **agent-remote-id**} ***number***

no session-limit agent-circuit-id | **session-limit agent-remote-id**

1.48.1 Purpose

Sets a limit to the number of sessions allowed for each subscriber line identified by an agent circuit ID or agent remote ID.

1.48.2 Command Mode

Subscriber configuration

1.48.3 Syntax Description

agent-circuit-id	Specifies session-limiting behavior based on the agent circuit ID.
agent-remote-id	Specifies session-limiting behavior based on the agent remote ID.
number	Specifies the maximum number of sessions allowed; ***number*** is a value between 1 and 255.

1.48.4 Default

By default, the SmartEdge router does not enforce a session limit.

1.48.5 Usage Guidelines

Use the **session-limit** command to set a limit to the number of sessions allowed for each subscriber line identified by an agent circuit ID or agent remote ID.

The SmartEdge router typically acquires an agent circuit ID or agent remote ID for a subscriber during the discovery process with a digital subscriber line access multiplexer (DSLAM) or dot1q PVC configuration.

Note: If the DSLAM or dot1q PVC configuration does not provide an agent circuit ID or agent remote ID, then the SmartEdge router does not enforce a configured session limit.

If a subscriber acquires an agent circuit ID and agent remote ID, the SmartEdge router checks for both session limits (if configured). If either check fails, the subscriber session fails.

A session limit is an attribute of a subscriber and exists within a local configuration. You can configure a session limit attribute within one of the following items:

- Subscriber name, which affects one subscriber
- Profile, which affects a custom group of subscribers
- Default profile, which affects all subscribers within a context

If several subscribers share a DSL service, you must configure the session limit attribute consistently for each subscriber to enforce the configured limit properly. The SmartEdge router checks the session limit for each subscriber when it authenticates the subscriber.

Use the **no** form of this command to remove a previously configured session limit and revert to the default behavior.

1.48.6 Examples

The following examples shows how to set a session limit by subscriber name. You enter a context and then enter each subscriber name and session limit attribute:

```
[local]Redback(config)#context isp2

[local]Redback(config-sub)#subscriber name alice

[local]Redback(config-sub)#session-limit agent-remote-id 2

[local]Redback(config-sub)#subscriber name bob

[local]Redback(config-sub)#session-limit agent-remote-id 2

[local]Redback(config-sub)#subscriber name connie

[local]Redback(config-sub)#session-limit agent-remote-id 2
```

1.49 set as-path

set as-path {**prepend** {*asn...* | *nn:nn...*} | **tag**}

no set as-path

1.49.1 Purpose

Prepends an autonomous system (AS) path to Border Gateway Protocol (BGP) routes that pass the route map conditions.

1.49.2 Command Mode

Route map configuration

1.49.3 Syntax Description

prepend	Increases the AS path by adding AS numbers (ASNs) to the AS path.
asn	ASN in integer format. The range of values is 1 to 65535. The subrange 64512 to 65535 is reserved for private autonomous systems. You can specify up to 16 ASNs. Each ASN must be separated by a space.
nn:nn	ASN in unsigned 4-byte *nn:nn* format, where the first *nn* represents the first 2 bytes of the ASN, and the second *nn* represents the second 2 bytes of the ASN. The range of values is 1 to 4294967295. You can specify up to 16 ASNs. Each ASN must be separated by a space.
tag	Sets the AS path to the value of the route tag.

1.49.4 Default

There are no preconfigured route map set actions. The AS path attribute for selected BGP routes is not modified.

1.49.5 Usage Guidelines

Use the **set as-path** command to prepend an AS path to BGP routes that pass the route map conditions. The only global BGP metric available to influence the best path selection is the AS path length. By varying the length of the AS path, a BGP peer can influence the best path selection. Usually the local AS number is prepended multiple times, increasing the AS path length.

Use the **no** form of this command to disable the configured set action.

1.49.6 Examples

The following example shows how to prepend **11** to all the routes advertised to **10.1.1.1:**

```
[local]Redback(config-ctx)#router bgp 11
[local]Redback(config-group)#neighbor 10.1.1.1
[local]Redback(config-peer)#route-map set-as-path out

.

.
[local]Redback(config-ctx)#route-map set-as-path
[local]Redback(config-route-map)#match as-path 1
[local]Redback(config-route-map)#set as-path prepend 11 11
```

1.50 set class

set class ***from-parameters to-attribute***

no set class ***from-parameters to-attribute***

1.50.1 Purpose

Assign a class from a set of parameters to an attribute.

1.50.2 Command Mode

Service profile configuration

1.50.3 Syntax Description

from-parameters	Parameter containing the class you want to assign to an attribute.
to-attribute	Attribute to which you want to assign a class.

1.50.4 Default

A class is not assigned to an attribute.

1.50.5 Usage Guidelines

Use the **set class** command to assign a class from a set of parameters to an attribute.

Use the **no** form of this command to remove an assigned class from an attribute.

1.50.6 Examples

The following example shows how to assign a class from a set of parameters called `$redir_class` to an attribute called `HTTP-Redirect-Rule:`

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

[local]Redback(config-ctx)# radius service profile Profile-HTTP-Redirect

[local]Redback(config-service-profile)# set class $redir_class HTTP-Redirect-Rule redirect
```

1.51 set community

set community {*community-num* [**no-export**] [**local-as**] [**no-advertise**] [**additive**] | **none**}

no set community

1.51.1 Purpose

Sets the Border Gateway Protocol (BGP) community attribute for routes that pass the route map conditions.

1.51.2 Command Mode

Route map configuration

1.51.3 Syntax Description

community-num	32-bit value expressed as either an unsigned decimal or in *nn*:*nn* format, where the first *nn* is the autonomous system number (ASN) and the second *nn* is a 2-byte number defined by the autonomous system. The range of unsigned decimal values is 1 to 4,294,967,295. The range of values for aa is 1 to 65,535. The range of values for either *nn* argument is 1 to 65,535. You can specify up to eight community numbers. Each entry must be separated by a space.
no-export	Optional. Does not advertise this route out of the local autonomous system (AS) confederation, or out of the local AS, if it is not part of a confederation.
local-as	Optional. Propagates this route only to peers in the local autonomous system. Does not send this route to external peers even if they are in the same confederation.
no-advertise	Optional. Does not advertise this route to any peer (internal or external).
additive	Optional. Adds the community to the existing communities.
none	Removes the community attribute from the prefixes that pass the route map conditions.

1.51.4 Default

There are no preconfigured route map set actions. The community attribute for selected BGP routes is not modified.

1.51.5 Usage Guidelines

Use the **set community** command to set the BGP community attribute for routes that pass the route map conditions. A community is a group of destinations that share some common attributes. Each destination can belong to multiple communities.

Use the **no** form of this command to disable the configured set action.

1.51.6 Examples

The following example shows how to ensure that routes that pass the AS path 1 conditions have the community set to **9**. Routes that pass the autonomous system path list **2** conditions have the community set to **no-export** (these routes are not advertised out of the local AS confederation, or out of the local AS, if it is not part of a confederation):

```
[local]Redback(config-ctx)#route-map set_community 10 permit
[local]Redback(config-route-map)#match as-path 1
[local]Redback(config-route-map)#set community 9

.

.

[local]Redback(config-ctx)#route-map set_community 20 permit
[local]Redback(config-route-map)#match as-path 2
[local]Redback(config-route-map)#set community no-export
```

1.52 set community-list

set community-list*ecl-name*delete

no set community-list

1.52.1 Purpose

Deletes Border Gateway Protocol (BGP) communities matching the community list from the BGP community attribute for routes that pass the route map conditions.

1.52.2 Command Mode

Route map configuration

1.52.3 Syntax Description

ecl-name	Name of the community list.
delete	Deletes communities that match the specified community list from the BGP community attribute.

1.52.4 Default

There are no preconfigured route map set actions. The community list for selected BGP routes is not modified.

1.52.5 Usage Guidelines

Use the **set community-list** command to delete BGP communities matching the community list from the BGP community attribute for routes that pass the route map conditions.

Use the **no** form of this command to disable BGP community deletion.

1.52.6 Examples

The following example shows how to delete communities in the community list, **comm06:**

```
[local]Redback(config-ctx)#route-map map04
[local]Redback(config-route-map)#match as-path-list aspath02
[local]Redback(config-route-map)#set community-list comm06 delete
```

1.53 set dampening

set dampening ***half-life reuse-threshold suppress-threshold max-suppress***

no set dampening

1.53.1 Purpose

Sets the Border Gateway Protocol (BGP) dampening policy for routes that pass the route map conditions.

1.53.2 Command Mode

Route map configuration

1.53.3 Syntax Description

half-life	Amount of time in minutes before a penalty is decreased by half. After a route is assigned a penalty, that penalty is decreased by half after each half-life period elapses. The range of values is 1 to 45 minutes.
reuse-threshold	Route is no longer suppressed when a route penalty level falls below this setting. The range of values is 1 to 20,000.
suppress-threshold	Route is suppressed when a route penalty level exceeds this setting. The range of values is 1 to 20,000.
max-suppress	Maximum amount of time in minutes a route can be suppressed. The range of values is 1 to 255.

1.53.4 Default

There are no preconfigured route map set actions. No route advertisement dampening is performed for selected routes.

1.53.5 Usage Guidelines

Use the **`set dampening`** command to set the BGP dampening policy for routes that pass the route map conditions.

Use the **`no`** form of this command to disable the configured set action.

1.53.6 Examples

The following example shows how to set the half life to **20** minutes, the reuse threshold to **800**, the suppress threshold to **2500**, and the maximum suppress time to **80** minutes:

```
[local]Redback(config-ctx)#route-map rmap_Q permit 10

[local]Redback(config-route-map)#match ip address prefix-list list1

[local]Redback(config-route-map)#set dampening 20 800 2500 80
```

1.54 set dscp

`set dscp` ***`dscp-value`***

`no set dscp`

1.54.1 Purpose

Sets the Differentiated Services Code Point (DSCP) value for routes that pass the route map conditions.

1.54.2 Command Mode

Route map configuration

1.54.3 Syntax Description

`dscp-value`	DSCP value. The range of values is 0 to 63.

1.54.4 Default

There are no preconfigured route map set actions. The DSCP value for selected routes are not modified.

1.54.5 Usage Guidelines

Use the **set dscp** command to set the DSCP value for routes that pass route-map conditions.

Border Gateway Protocol (BGP) destination-based quality of service (QoS) supports setting the DSCP byte for IP traffic based on BGP attributes including community list and AS path. This can be used by a service provider (SP) to provide multiple levels of service based on a customers IP destination. BGP routes can be assigned a DSCP value based on the BGP table map, route map. When a packet is received on an interface with **mark dscp destination** enabled, and the packet is routed using a route with an associated DSCP, the packet's DCSP is updated and the IP header checksum is recalculated.

Use the **no** form of this command to disable the configured set action.

1.54.6 Examples

The following example shows how to set the DCSP value to **5** for routes passing IP access control list **23** conditions:

```
[local]Redback(config-ctx)#route-map map12 permit 10

[local]Redback(config-route-map)#match ip access-list 23

[local]Redback(config-route-map)#set dscp 5
```

1.55 set ext-community

set ext-community {*ext-community-num* [**additive**] | **none**}

no set ext-community

1.55.1 Purpose

Sets the Border Gateway Protocol (BGP) extended community attribute for routes that pass the route map conditions.

1.55.2 Command Mode

Route map configuration

1.55.3 Syntax Description

ext-community-num	Extended community number, which can be specified only when configuring an extended community list. It can be expressed in either of the following formats: • *tt*:*asn*:*nnnn*, where *tt* is the extended community type, *asn* is the ASN, and *nnnn* is either a 32-bit integer or a 16-bit integer, depending on the size of the ASN. The extended community type identifies either a target or origin community. The target community identifies the destination to which the route is going, and the origin community identifies source from where the route originated. The *tt* argument is a placeholder for either the **ro** (route origin) keyword, or the **rt** (route target) keyword. You can specify the ASN as either a two-byte (two-octet) or four-byte (four-octet) integer. A value of 65535 or lower is interpreted as a two-byte integer, unless you add an **L** suffix (for example, **125L**), in which case it is interpreted as a four-byte integer. A value larger than 65535 is always interpreted as a four-byte integer, and the **L** suffix is optional. If the ASN is two-bytes, then *nnnn* is a 32-bit integer. If the ASN is four-bytes, then *nnnn* is a 16-bit integer. • *tt*:*ip-addr*:*nn*, where *tt* is the extended community type, *ip-addr* is the IP address in the form *A.B.C.D*, and *nn* is a 16-bit integer.
additive	Optional. Adds the specified extended community numbers to the extended community. You can specify up to eight extended community numbers. Each entry must be separated by a space.
none	Removes the extended community attribute from the routes that pass the route map conditions.

1.55.4 Default

There are no preconfigured route map set actions. The extended community attribute for selected BGP routes is not modified.

1.55.5 Usage Guidelines

Use the **set ext-community** command to set the BGP extended community attribute for routes that pass the route map conditions.

An extended community is a group of destinations that share some common attributes. Each destination can belong to multiple extended communities. Up to eight extended communities can be specified. If the **`additive`** keyword is used, extended communities are added to the existing BGP extended community list; however, unlike AS path attributes, extended community attributes do not include duplicate entries.

Note: Up to 300 BGP extended communities can be added to a route by using the **`continue`** command in a route map to execute multiple **`set ext-community`** commands.

You cannot configure the route origin at both the address family level and the BGP neighbor level.

If you aggregate routes containing extended communities, the extended community information for each individual route is lost. You can apply the BGP extended communities attribute to the aggregated route using the **`set ext-community`** command.

Use the **`no`** form of this command to disable the configured set action.

1.55.6 Examples

The following example shows how to ensure that routes that pass the autonomous system (AS) path list **1** conditions have their extended community attribute set to **rt:10.10.10.1:15:**

```
[local]Redback(config-ctx)#route-map set_ext_community 10 permit
[local]Redback(config-route-map)#match as-path 1
[local]Redback(config-route-map)#set ext-community rt:10.10.10.1:15
```

The following example shows how to ensure that routes that pass the AS path list **2** conditions have their extended community attribute removed:

```
[local]Redback(config-ctx)#route-map set_ext_community 20 permit
[local]Redback(config-route-map)#match as-path 2
[local]Redback(config-route-map)#set ext-community none
```

1.56 set ip aggregate

`set ip aggregate` ***`prefix-list-name`***

`no set ip aggregate`

1.56.1 Purpose

Specifies that IPv4 routes that are selected for redistribution and match the specified IPv4 prefix are summarized (rather than individually redistributed).

1.56.2 Command Mode

Route map configuration

1.56.3 Syntax Description

prefix-list-name	Identifies an IPv4 prefix list.

1.56.4 Default

There are no preconfigured route map set actions.

1.56.5 Usage Guidelines

Use the **set ip aggregate** command to specify that IPv4 routes that are selected for redistribution and match the specified IPv4 prefix are summarized (rather than individually redistributed). Only the prefix and prefix length from the prefix list entries are summarized; for routes containing the prefix and prefix length, only the aggregate is redistributed, rather than the route itself.

For each summarized prefix, a reject route (a route with a NULL0 next-hop) is added to the RIB. The default administrative distance for this reject route is 254.

Note: When an IP prefix list is used for aggregation, the **ge** and **le** parameters (configured with the **seq** command) are ignored, and the prefix list entries match any route subsumed by the prefix. In such cases, the **ge** parameter is implicit.

Use the **no** form of this command to disable the configured set action.

1.56.6 Examples

The following example shows how to specify that IPv4 routes that are selected for redistribution and match the specified IPv4 prefix are summarized:

```
[local]Redback(config-ctx)#route-map rmap_Q permit 10

[local]Redback(config-route-map)#match ip address prefix-list pl1

[local]Redback(config-route-map)#set ip aggregate test-list
```

1.57 set ipv6 aggregate

```
set ipv6 aggregate prefix-list-name
```

```
no set ipv6 aggregate
```

1.57.1 Purpose

Specifies that IPv6 routes that are selected for redistribution and match the specified IPv6 prefix are summarized (rather than individually redistributed).

1.57.2 Command Mode

Route map configuration

1.57.3 Syntax Description

prefix-list-name	Identifies an IPv6 prefix list.

1.57.4 Default

There are no preconfigured route map set actions.

1.57.5 Usage Guidelines

Use the **set ipv6 aggregate** command to specify that IPv6 routes that are selected for redistribution and match the specified IPv6 prefix are summarized (rather than individually redistributed). Only the prefix and prefix length from the prefix list entries are summarized; for routes containing the prefix and prefix length, only the aggregate is redistributed, rather than the route itself.

For each summarized prefix, a reject route (a route with a NULL0 next-hop) is added to the RIB. The default administrative distance for this reject route is 254.

Note: When an IPv6 prefix list is used for aggregation, the **ge** and **le** parameters (configured with the **seq** command) are ignored and the prefix list entries match any route subsumed by the prefix. In such cases, the **ge** parameter is implicit.

Use the **no** form of this command to disable the configured set action.

1.57.6 Examples

The following example shows how to specify that IPv6 routes that are selected for redistribution and match the specified IPv6 prefix are summarized (rather than individually redistributed):

```
[local]Redback(config-ctx)#route-map rmap_Q permit 10

[local]Redback(config-route-map)#match ipv6 address prefix-list pl1

[local]Redback(config-route-map)#set ipv6 aggregate ipv6-list
```

1.58 set ip next-hop

set ip next-hop {*ip-addr* | **peer-address** | **prefix-address**}

no set ip next-hop

1.58.1 Purpose

Determines the next-hop IP address used to forward packets for routes that pass the route map conditions.

1.58.2 Command Mode

route map configuration

1.58.3 Syntax Description

ip-addr	Next-hop IP address in the form ***A.B.C.D***.
peer-address	Sets the next-hop IP address to a Border Gateway Protocol (BGP) peer address. For an inbound route map, the system uses the IP address of the BGP neighbor's peer. For an outbound route map, the system uses the IP address of the local BGP peer.
prefix-address	Sets the next-hop IP address to match the IPv4 prefix address of the host. Only /32 prefixes are valid. Be aware that the **prefix-address** settings take effect only if the prefix is IPv4 unicast, the prefix length is 32, and the route map is applied with the *redistribute* (IPv4) command under BGP address family configuration mode.

1.58.4 Default

There are no preconfigured route map set actions. The next hops of selected routes are not modified.

1.58.5 Usage Guidelines

Use the **set ip next-hop** command to determine the next-hop IP address used to forward packets for routes that pass the route map conditions. If the **peer-address** keyword is applied to an inbound route map, the next hop of received matching routes is set to the IP address of the BGP neighbor's peer, overriding any third-party next hops. If the **peer-address** keyword is applied to an outbound route map, the next hop of the advertised matching routes is set to the IP address of the local BGP speaker, thus disabling the next-hop calculation.

Note: Be aware that the **prefix-address** settings take effect only if the prefix is IPv4 unicast, the prefix length is 32, and the route map is applied with the *redistribute* (IPv4) command under BGP address family configuration mode.

Use the **no** form of this command to disable the configured set action.

1.58.6 Examples

The following example shows how to set the next hop for routes passing IP access list **1** to the BGP neighbor's peer IP address:

```
[local]Redback(config-ctx)#route-map rmap_Q permit 10

[local]Redback(config-route-map)#match ip access-list 1

[local]Redback(config-route-map)#set ip next-hop peer-address
```

The following example shows how to set the next-hop IP address to match the IPv4 prefix address of the host. This example assumes there is an OSPF route 1.2.3.4/32 that has a nexthop of 5.6.7.8. First, the user configures a route map called `mymap` that:

- Permits routes with a destination IP address that matches the addresses specified in the prefix list mylist
- Sets the next-hop IP address to match the IPv4 prefix address of the host

Next, the user redistributes OSPF routes into BGP using the settings in the `mymap` route map:

```
[local]Redback(config-ctx)#route-map mymap permit 10

[local]Redback(config-route-map)#match ip address prefix-list mylist

[local]Redback(config-route-map)#set ip next-hop prefix-address

[local]Redback(config-route-map)#exit

[local]Redback(config-ctx)#router bgp 1

[local]Redback(config-bgp)#address-family ipv4 unicast

[local]Redback(config-bgp-af)#redistribute ospf route-map mymap
```

The following example shows how to use the **`show bgp route`** command to verify the configuration. The OSPF route `1.2.3.4/32` (which originally had the nexthop `5.6.7.8`) is redistributed into BGP with the nexthop `1.2.3.4`:

```
[local]Redback(config-bgp)#show bgp route

Address Family: ipv4 unicast
BGP table version is 18, local router ID is 99.99.99.1 Status codes: d damped, h history, > best,
I internal Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop                Metric  LocPrf  Weight Path
 >  1.2.3.4/32         1.2.3.4                     11     100   32768 ?
============================
```

1.59 set ipv6 next-hop

`set ipv6 next-hop` {*`ipv6-addr`* | **`peer-address`**}

`no set ipv6 next-hop`

1.59.1 Purpose

Determines the next-hop IP Version 6 (IPv6) address used to forward packets for routes that pass the route map conditions.

1.59.2 Command Mode

route map configuration

1.59.3 Syntax Description

`ipv6-addr`	Next-hop IPv6 address in the form ***`A:B:C:D:E:F:G`***.
`peer-address`	Sets the next-hop IPv6 address to a Border Gateway Protocol (BGP) peer address. For an inbound route map, the system uses the IPv6 address of the BGP neighbor's peer. For an outbound route map, the system uses the IPv6 address of the local BGP peer.

1.59.4 Default

There are no preconfigured route map set actions. The next hops of selected routes are not modified.

1.59.5 Usage Guidelines

Use the **`set ipv6 next-hop`** command to determine the next-hop IPv6 address used to forward packets for routes that pass the route map conditions. If you apply the **`peer-address`** keyword to an inbound route map, the next hop of received matching routes is set to the IPv6 address of the BGP neighbor's peer, overriding any third-party next hops. If you apply the **`peer-address`** keyword to an outbound route map, the next hop of the advertised matching routes is set to the IPv6 address of the local BGP speaker, thus disabling the next-hop calculation.

Use the **`no`** form of this command to disable the configured set action.

1.59.6 Examples

The following example shows how to set the next hop for routes passing IPv6 access list **1** to the BGP neighbor's peer IPv6 address:

```
[local]Redback(config-ctx)#route-map rmap_Q permit 10

[local]Redback(config-route-map)#match ip access-list 1

[local]Redback(config-route-map)#set ipv6 next-hop peer-address
```

1.60 set label

`set label`

`no set label`

1.60.1 Purpose

Sets the Multiprotocol Label Switching (MPLS) label for routes that pass the route map conditions.

1.60.2 Command Mode

route map configuration

1.60.3 Syntax Description

This command has no keywords or arguments.

1.60.4 Default

There are no predefined route map set actions. The label for the route is unmodified.

1.60.5 Usage Guidelines

Use the `set label` command to set the MPLS label for routes that pass the route map conditions.

Use the `no` form of this command to remove the MPLS label setting.

1.60.6 Examples

The following example shows how to set the MPLS label for routes that pass the conditions specified by the route map, **r1**:

```
[local]Redback(config-ctx)#route-map r1

[local]Redback(config-route-map)#set label

[local]Redback(config-route-map)#
```

1.61 set level

set level {**level-1** | **level-1-2** | **level-2** | **nssa-areas** | **transit-areas**}

no set level

1.61.1 Purpose

For routes that pass the route map conditions, sets the advertisement scope for routes redistributed into Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) routing domains.

1.61.2 Command Mode

route map configuration

1.61.3 Syntax Description

`level-1`	Redistributes routes into IS-IS level 1 areas. Routes are not advertised in IS-IS level 2 areas.
`level-1-2`	Redistributes routes into IS-IS level 1 and level 2 areas.
`level-2`	Redistributes routes into IS-IS level 2 areas. Routes are not advertised in IS-IS level 1 areas.
`nssa-areas`	Redistributes routes into OSPF not-so-stubby-areas (NSSAs). Routes are not advertised in OSPF transit areas.
`transit-areas`	Redistributes routes into OSPF transit areas. Routes are not advertised in OSPF NSSAs.

1.61.4 Default

There are no preconfigured route map set actions. For OSPF, routes are advertised into both regular and transit areas. For IS-IS, routes are advertised into both level 1 and level 2 areas.

1.61.5 Usage Guidelines

Use the **`set level`** command to set the advertisement scope for routes redistributed into OSPF and IS-IS routing domains.

Use this command in conjunction with the **`route-map`** command in context configuration mode, with the **`redistribute`** command in OSPF router configuration mode, and with the **`redistribute`** command in IS-IS configuration mode.

When a redistributed route is advertised into an OSPF transit area, it is advertised as a type 5 link-state advertisement (LSA). When a redistributed route is advertised into an OSPF NSSA, it is advertised as a type 7 LSA. When the **`nssa-area`** keyword is specified for a router that is part of an NSSA, but is not an area border router (ABR), the corresponding routes are advertised as type 7 LSAs without the P (propagate) bit set. The propagate bit is described in RFC 1587, ***`The OSPF NSSA Option`***.

Use the **`no`** form of this command to return the system to its default behavior.

1.61.6 Examples

The following example shows how to limit the redistribution of static routes into OSPF transit areas:

```
[local]Redback(config-ctx)#route-map no-nssa-areas permit 10
[local]Redback(config-route-map)#set level transit-areas
[local]Redback(config-route-map)#exit
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#redistribute static route-map no-nssa-areas
```

1.62 set local-preference

set local-preference ***local-pref***

no set local-preference

1.62.1 Purpose

Sets the degree of preference for the Border Gateway Protocol (BGP) autonomous system (AS) path for routes that pass the route map conditions.

1.62.2 Command Mode

route map configuration

1.62.3 Syntax Description

local-pref	Integer. The range of values is 0 to 4,294,967,295; the default value is 100.

1.62.4 Default

There are no preconfigured route map set actions. The preference value is for BGP routes is 100.

1.62.5 Usage Guidelines

Use the **set local-preference** command to set the degree of preference for the BGP AS path for routes that pass the route map conditions. The preference is sent only to routers in the local autonomous system. A route with a high value is preferred over a route with a lower value.

Use the **no** form of this command to disable the configured set action.

1.62.6 Examples

The following example shows how to set the local preference for all routes included in route access list **1** to **50:**

```
[local]Redback(config-ctx)#route-map rmap_P
[local]Redback(config-route-map)#match route-access-list 1
[local]Redback(config-route-map)#set local-preference 50
```

1.63 set metric

set metric [+ | -] ***metric***

no set metric

1.63.1 Purpose

Sets, increments, or decrements the metric value for the destination routing protocol for routes that pass the route map conditions.

1.63.2 Command Mode

route map configuration

1.63.3 Syntax Description

+	Optional. Adds the specified metric value.
-	Optional. Subtracts the specified metric value.
metric	Metric value. The range of values is 0 to 4,294,967,295.

1.63.4 Default

There are no preconfigured route map set actions. The metric for selected routes is not modified. The metric value is determined by the application and routing protocol.

1.63.5 Usage Guidelines

Use the **set metric** command to set, increment, or decrement the metric value for the destination routing protocol for routes that pass the route map conditions.

Use the **no** form of this command to disable the configured metric value.

1.63.6 Examples

The following example shows how to set the metric value for the routing protocol to **50:**

```
[local]Redback(config-ctx)#route-map rmap_M
[local]Redback(config-route-map)#set metric 50
```

The following example shows how to add **11** to the metric value for the routing protocol:

```
[local]Redback(config-ctx)#route-map add_metric permit 20
[local]Redback(config-route-map)#set metric +11
```

1.64 set metric-type

set metric-type {**external** | **internal** | **type-1** | **type-2**}

no set metric-type

1.64.1 Purpose

Sets the metric type for the destination routing protocol for routes that pass the route map conditions.

1.64.2 Command Mode

route map configuration

1.64.3 Syntax Description

external	Specifies the Intermediate System-to-Intermediate System (IS-IS) external metric.
internal	Specifies the Internal Gateway Protocol (IGP) as the Multi-Exit Discriminator (MED) for Border Gateway Protocol (BGP).
type-1	Specifies the Open Shortest Path First (OSPF) external Type 1 metric.
type-2	Specifies OSPF external Type 2 metric.

1.64.4 Default

There are no preconfigured route map set actions. The metric type for selected routes is not modified. For routes redistributed into OSPF, the default metric is Type 2.

1.64.5 Usage Guidelines

Use the **set metric-type** command to set the metric type for the destination routing protocol for routes that pass the route map conditions.

Use the **no** form of this command to disable the configured set action.

1.64.6 Examples

The following example shows how to set the metric type to **external:**

```
[local]Redback(config-ctx)#route-map rmap_M
[local]Redback(config-route-map)#set metric-type external
```

1.65 set origin

set origin {**egp** | **igp** | **incomplete**}

no set origin

1.65.1 Purpose

Sets the origin of the Border Gateway Protocol (BGP) path for routes that pass the route map conditions.

1.65.2 Command Mode

route map configuration

1.65.3 Syntax Description

`egp`	Indicates that the path information originated from another autonomous system (AS).
`igp`	Sets the origin to the local Interior Gateway Protocol (IGP).
`incomplete`	Indicates that the origin is unknown.

1.65.4 Default

There are no preconfigured route map set actions. The origin for selected BGP routes is not modified. The origin is determined by the route type.

1.65.5 Usage Guidelines

Use the **set origin** command to set the BGP origin path for routes that pass the route map conditions.

Use the **no** form of this command to disable the configured set action.

1.65.6 Examples

The following example shows how to set the origin of routes that pass the route map conditions to **IGP:**

```
[local]Redback(config-ctx)#route-map rmap_H

[local]Redback(config-route-map)#match route-access-list 10

[local]Redback(config-route-map)#set origin igp
```

1.66 set-overload-bit

set-overload-bit [**on-startup** [*interval*] | **bgp-converge-delay** [*interval*] | **strict-bgp-tracking**]

no set-overload-bit

1.66.1 Purpose

Sets the overload bit so that other devices do not use the SmartEdge router to forward traffic.

1.66.2 Command Mode

IS-IS router configuration

1.66.3 Syntax Description

`on-startup`	Optional. Sets the overload bit on startup, and continues until the timer expires.
`interval`	Optional. Timer interval in seconds. The range of values is 10 to 3,600 seconds; the default value is 210 seconds.
`bgp-converge-delay`	Optional. Sets the overload bit on startup, and continues until timer expires or the Border Gateway Protocol (BGP) converges. The overload bit is removed as soon as BGP converges.
`strict-bgp-tracking`	Optional. Sets the overload bit until BGP converges. If BGP is not converged or not running, the overload bit remains set. There is no time out for the overload bit as long as BGP is not converged.

1.66.4 Default

The overload bit is not set.

1.66.5 Usage Guidelines

Use the **`set-overload-bit`** command to set the overload bit so that other devices do not use the SmartEdge router to forward traffic. The other routers in the domain can still forward traffic to IP networks directly connected to this router.

The overload bit is designed by the Intermediate System-to-Intermediate System (IS-IS) protocol to indicate a router overload condition, such as memory shortage; however, this overload bit can be manually set or dynamically set for other network conditions. For example, when a router resides in a web server location, it may only want to attract traffic destined to the web servers, and not attract general traffic headed to other routers. When BGP is running on the router, and if it is not fully converged, the router may not have all the routing information for transit traffic.

Use the **`set-overload-bit`** command without any option to indefinitely set the overload bit. This is suitable for the web server location example above.

Use the **`on-startup`** keyword if BGP is not configured on the router, or if BGP convergence is not an issue. When the router starts, IS-IS temporarily sets the overload bit to allow the router to reach full functionality with complete routing information on the router.

Use the **`bgp-converge-delay`** keyword if BGP is not fully converged, and you want to use the IS-IS overload bit feature to delay other routers from sending transit traffic through the router until BGP converges. If the BGP converge delay time expires, the overload bit is removed, even if BGP has not converged; therefore, you should adjust the BGP converge delay time so that it is appropriate to your network size and the amount information in the BGP routing table.

Use the **`strict-bgp-tracking`** keyword if BGP is not fully converged, and you want to use the overload bit feature to stop other routers from sending transit traffic through the router to until BGP converges. The overload bit is removed only when full BGP convergence is reached.

Use the **`no`** form of this command to remove the overload bit.

1.66.6 Examples

The following example shows how to enable ISIS to use the overload bit to delay transit traffic for **60** seconds:

```
[local]Redback(config-ctx)#router isis test

[local]Redback(config-isis)#set-overload-bit bgp-converge-delay 60
```

1.67 set tag

`set tag` ***`tag`***

`no set tag`

1.67.1 Purpose

Sets the route tag value for routes that pass the route map conditions.

1.67.2 Command Mode

route map configuration

1.67.3 Syntax Description

`tag`	Route tag value. An unsigned 32-bit integer, the range of values is 1 to 4,294,967,295; the default value is 0.

1.67.4 Default

There are no preconfigured route map set actions. The route tag for selected routes is not modified.

1.67.5 Usage Guidelines

Use the **set tag** command to set the route tag value for routes that pass the route map conditions.

Use the **no** form of this command to remove the route tag setting.

1.67.6 Examples

The following example shows how to set the route tag to **8** for routes that pass the route map conditions:

```
[local]Redback(config-ctx)#route-map map_F

[local]Redback(config-route-map)#set tag 8
```

1.68 set traffic-index

set traffic-index *value*

no set traffic-index

1.68.1 Purpose

Sets the traffic index value for routes that pass the route map conditions.

1.68.2 Command Mode

route map configuration

1.68.3 Syntax Description

value	Traffic index number. The range of values is 1 to 8.

1.68.4 Default

There are no preconfigured route map set actions. The traffic-index for selected routes is not modified.

1.68.5 Usage Guidelines

Use the **set traffic-index** command to set the traffic index value for routes that pass the route map conditions.

Per index counters for interfaces with Border Gateway Protocol (BGP) attribute-based accounting enabled are maintained for BGP routes assigned a traffic index. The byte and packet counters for a traffic index are incremented based on the route traversed by IP traffic received on the ingress interface. For more information, see the **traffic-index-accounting** command, and the **table-map** command in *Command List*.

Use the **no** form of this command to remove the traffic index setting.

1.68.6 Examples

The following example shows how to set the traffic index to **3** for routes that pass the route map conditions:

```
[local]Redback(config-ctx)#route-map bgp-accounting permit 10

[local]Redback(config-route-map)#set traffic-index 3
```

1.69 set weight

set weight ***weight***

no set weight

1.69.1 Purpose

Sets the degree of preference for Border Gateway Protocol (BGP) routes that pass the route map conditions.

1.69.2 Command Mode

route map configuration

1.69.3 Syntax Description

weight	Weight value of a specified BGP route. The range of values is 0 to 65,535.

1.69.4 Default

There are no preconfigured route map set actions. The weight for selected BGP routes is not modified.

1.69.5 Usage Guidelines

Use the **`set weight`** command to set the degree of preference for BGP routes that pass the route map conditions. A route with a high value is preferred over a route with a lower value.

Use the **`no`** form of this command to disable the configured set action.

1.69.6 Examples

The following example shows how to set the BGP weight to **50** for routes that are permitted by route access list **10:**

```
[local]Redback(config-ctx)#route-map rmap_G
[local]Redback(config-route-map)#match route-access-list 10
[local]Redback(config-route-map)#set weight 50
```

1.70 sham-link

`sham-link` ***`src-addr dest-addr`***

`no sham-link` ***`src-addr dest-addr`***

1.70.1 Purpose

Creates an Open Shortest Path First (OSPF) adjacency tunneled over a Virtual Private Network (VPN) backbone and enters OSPF sham link configuration mode.

1.70.2 Command Mode

OSPF area configuration

1.70.3 Syntax Description

src-addr	Source IP address used as the local endpoint for the sham link. It must be the address of a local loopback interface.
dest-addr	Destination IP address used as the remote endpoint for the sham link.

1.70.4 Default

No OSPF sham links are configured.

1.70.5 Usage Guidelines

Use the **sham-link** command to create an OSPF adjacency tunneled (sham link) over a VPN backbone and enters OSPF sham link configuration mode. Sham links allow the VPN backbone path to be preferred when there are intra-area backdoor links between customer edge (CE) routers in the VPN.

The local connected route corresponding to the source IP address for the sham link must be redistributed into Border Gateway Protocol (BGP) and advertised over the VPN infrastructure to a provider edge (PE) router containing the other end of the sham link.

The route corresponding the remote end of the sham link must be redistributed into the corresponding OSPF instance in the VPN context. VPN routing must be enabled for the OSPF instance.

The cost of the sham link can be configured or will inherit the BGP Multi-Exit Discriminator (MED) from the VPN route.

Use the **no** form of this command to remove the sham link.

For more information on sham links, see the Internet Draft, `OSPF as the PE/CE Protocol in BGP/MPLS VPNs`, draft-rosen-vpns-ospf-bgp-mpls-04 .txt.

1.70.6 Examples

The following example shows how to configure a sham link with cost **10** in area **0** for the OSPF instance within the VPN context:

```
[local]Redback(config-ospf)#vpn domain-id 1.1.1.1 domain-tag 0xfeedacee
[local]Redback(config-ospf)#area 0.0.0.0
[local]Redback(config-ospf-area)#sham-link 1.1.1.1 2.2.2.2
[local]Redback(config-ospf-sham-link)#cost 10
[local]Redback(config-ospf-sham-link)#exit
[local]Redback(config-ospf)#redistribute bgp 1000
```

1.71 shaping

shaping {**cbr rate** *rate* **cdvt** *cdvt* | **ubr** [**pcr** *pcr* | **weight** *weight*] | **ubre mcr** *mcr* **pcr** *pcr* **bt** *bt* | **vbr-nrt pcr** *pcr* **cdvt** *cdvt* **scr** *scr* **bt** *bt* | **vbr-rt pcr** *pcr* **cdvt** *cdvt* **scr** *scr* **bt** *bt*}

default shaping

1.71.1 Purpose

Specifies the corresponding traffic class to use for any Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) or shaped virtual path (VP) that references this profile.

1.71.2 Command Mode

ATM profile configuration

1.71.3 Syntax Description

cbr	Specifies traffic class based on a constant bit rate (CBR).
rate *rate*	Traffic bit rate in kbps. The range of values is 64 to 599,040.
cdvt *cdvt*	Cell delay variation tolerance (CDVT), defined as the maximum cell delay in microseconds between the expected arrival time and the actual arrival time. It controls how much cell clustering is allowed. The range of values is 1 to 10,000.
ubr	Configures traffic class based on an unspecified bit rate (UBR).
pcr *pcr*	Optional. Peak cell rate (PCR); the upper limit on traffic in kbps, that can be applied to an ATM connection. The range of values is 65 to 599,040, but it must be greater than the value specified for MCR, if specified. Optional for the UBR traffic class; required for the UBRe traffic class.

weight ***weight***	Optional. Weight, in number of ATM cells, to assign to any shaped VP or PVC; applicable only to VPs and PVCs on second-generation ATM OC traffic cards in VC fairness mode. This option is ignore otherwise. The range of values is 1 to 32,000 cells; the default value is 4 cells.
ubre	Configures traffic class based on an unspecified bit rate extended (UBRe) that guarantees the specified MCR and allows bursts up to the specified PCR.
mcr ***mcr***	Minimum cell rate (MCR); specifies lower limit on traffic in kbps, that can be applied to an ATM connection. The range of values is 64 to 599,039, but it must be less than the value specified for PCR.
bt ***bt***	Burst tolerance (BT); specifies the number of microseconds that traffic can be transmitted at the peak cell rate. The range of values is 1 to 10,000.
vbr-nrt	Configures traffic class based on variable bit rate-nonrealtime (VBR-nrt).
scr ***scr***	Sustained cell rate (SCR); specifies the rate in kbps that should be maintained during transmission of cells across a particular ATM connection. The range of values is 64 to 599,040.
vbr-rt	Configures traffic class based on variable bit rate-realtime (VBR-rt).

1.71.4 Default

Shaping is UBR with the maximum line rate.

1.71.5 Usage Guidelines

Use the **shaping** command to specify the corresponding traffic class to use for any ATM PVC or VP that references this profile. The following traffic classes are supported:

- Constant bit rate (CBR)—CBR supports realtime applications that are sensitive to delay variations; for example, voice and video.
- Unspecified bit rate (UBR)—UBR is the simplest type of traffic class. It provides no specific quality of service or guaranteed throughput. UBR mode is typically used to carry LAN and WAN traffic.

  You can optionally allow bursts of traffic up to a specified peak cell rate (PCR); PCR is the maximum rate at which traffic can be sent, measured in kbps. If PCR is not specified, the default value is the line rate.
- Unspecified bit rate-extended (UBRe)—UBRe distributes otherwise unused bandwidth across designated connections. If there is sufficient traffic it

guarantees the specified minimum cell rate (MCR) and allows bursts up to the PCR.

Note: UBRe is available only for ATM PVCs configured on ports on second-generation ATM OC traffic cards. It is not available for shaped VPs or PVCs on these cards under either of the following conditions: The VP or PVC has a QoS ATMWFQ policy attached. The PVC is configured on a shaped VP and the card has the ATM priority segmentation and reassembly (SAR) image loaded.

- Variable bit rate nonrealtime (VBR-nrt)—VBR-nrt supports applications that have variable rate, bursty traffic characteristics. This traffic class is suitable for critical data applications.
- Variable bit rate realtime (VBR-rt)—VBR-rt supports time-sensitive applications that also require constrained delay and delay variation; for example, compressed audio.

Note: For more configuration guidelines for ATM profiles, VPs, and PVCs with regard to traffic classes, see *ATM Configuration Guidelines*.

Successive **`shaping`** commands replace the previous shaping configuration for the profile.

PVCs shaped with VBR-rt or VBR-nrt can experience performance limitations when other PVCs on the same port are configured with other traffic classes. To avoid these limitations, the following settings are recommended for both VBR traffic classes:

- When the sustainable cell rates (SCR) is less than 50% of line rate, set the peak cell rate (PCR) to 50% of the usable bandwidth and set the burst tolerance (BT) to a value greater than 20 microseconds.
- When SCR is set between 50% and 100% of the usable bandwidth, set the PCR to 100% of the usable bandwidth and the BT to a value greater than 20 microseconds.
- VBR shaping requires the ability to increase the cell rate during a specified period. This burst period is proportional to the difference between the specified values for the PCR and SCR. Setting the values to be equal implies that no burst period is allowed. In most cases, the PCR should exceed the SCR value by a minimum of 20% of the usable bandwidth. When the PCR and SCR values are equal, the SARC switches to an enhanced VBR shaping algorithm. This algorithm provides shaping behavior similar to CBR, and the system does not display an error message.
- **Note:** No burst period is allowed when the values for the PCR and SCR are equal; in this case, the BT has no effect on VBR shaping behavior.

The aggregated transmit rates for all ATM PVCs on a port must be less than its usable bandwidth or its oversubscribed bandwidth, whichever is larger. You can oversubscribe the bandwidth of an ATM port using the **over-subscription-rate** command in ATM OC configuration mode.

Note: The usable bandwidth (the effective speed for user traffic) of a port is displayed by the show port detail command in any mode.

Use the **default** form of this command to specify the default shaping.

1.71.6 Examples

The following example shows how to specify the **vbr-nrt** traffic class for an ATM profile with a PCR of **2500** kbps; a CDVT of **20** ms; an SCR of **2400** kbps; and a BT of **10** ms:

```
[local]Redback(config)#atm profile low_rate
[local]Redback(config-atm-profile)#shaping vbr-nrt pcr 2500 cdvt 20 scr 2400 bt 10
```

1.72 shaping-profile

shaping-profile ***atm-prof-name***

no shaping-profile

1.72.1 Purpose

Assigns an Asynchronous Transfer Mode (ATM) profile to the subscriber record or profile.

1.72.2 Command Mode

subscriber configuration

1.72.3 Syntax Description

atm-prof-name	Name of an existing ATM profile.

1.72.4 Default

A subscriber session that is initiated on an ATM permanent virtual circuit (PVC) is governed by the ATM profile assigned to the PVC.

1.72.5 Usage Guidelines

Use the **`shaping-profile`** command to assign an ATM profile to the subscriber record or profile.

Note: The ATM profile must exist or the subscriber session is not initiated.

Use the **`no`** form of this command to remove the ATM profile from the subscriber record or profile; a subscriber session initiated on an ATM PVC will be governed by the ATM profile assigned to that ATM PVC.

1.72.6 Examples

The following example shows how to assign the ATM profile, **ubr**, to the named subscriber profile, **isp2:**

```
[local]Redback(config-ctx)#subscriber profile isp2

[local]Redback(config-sub)#shaping-profile ubr
```

1.73 show aaa route-download

`show aaa route-download`

1.73.1 Purpose

Displays configuration and operational status for route downloads.

1.73.2 Command Mode

exec

1.73.3 Default

None

1.73.4 Examples

The following information is displayed when you run the **`show aaa route-download`** command:

```
[local]Redback#show aaa route-download

Method                              : radius
Download interval                   : 4200 secs
Synchronization time                : <NOT SET>
Default cost                        : 0
Username prefix                     : PE1
Password                            : redback
Status                              : idle
Last download attempt               : Tue Jun 15 23:28:39 2010
Last successful download            : Tue Jun 15 23:28:45 2010
Next scheduled download             : Wed Jun 16 00:11:27 2010
```

1.74 show aaa route-download statistics

show aaa route-download statistics

1.74.1 Purpose

Displays statistics related to route downloads.

1.74.2 Command Mode

exec

1.74.3 Default

None

1.74.4 Examples

The following information is displayed when you run the **show aaa route-download statistics** command:

```
[local]Redback#show aaa route-download statistics
```

```
Total download attempts              : 1
Total manual download attempts       : 1
Total route reload attempts          : 0
Total route clear attempts           : 0
Successful downloads                 : 1
Failed downloads                     : 0
Cancelled downloads                  : 0
In progress downloads                : 0
Total downloaded fragments           : 1334
Total downloaded routes              : 40020
Total modified routes                : 0

Error statistics
================
        Timeout                       : 0
        Bad packet                    : 0
        Config error                  : 0
        Invalid context               : 0
        Unclassified                  : 0
```

For “global” method, only the following statistics are applicable; others are not applicable:

```
Total route reload attempts
Total route clear attempts
Total modified routes
```

1.75 show aaa route subscriber aggregate

`show aaa route subscriber aggregate`

1.75.1 Purpose

Displays all the routes present in the AAA daemon. It does not display transient downloaded routes.

1.75.2 Command Mode

exec

1.75.3 Default

None

1.75.4 Examples

The following information is displayed when you run the **show aaa route subscriber aggregate** command:

```
[local]Redback#show aaa route subscriber aggregate
1.1.0.0/16 null0 0
2.1.0.0/24 null0 0
3.1.0.0/26 null0 0
130.248.0.0/14 null0 0
22:0:0:757::1/64 null0 22
23:0:0:757::1/32 null0 23
24:0:0:757::1/96 null0 24
25:0:0:757::1/48 null0 25
26:0:0:757::1/64 null0 26
27:0:0:757::1/64 null0 27
```

1.76 show access-group

To display general information about all configured access control lists (ACLs), the syntax is:

show access-group

To display information about IPv4 filtering ACLs that are applied to subscriber profiles or records, the syntax is:

show access-group subscriber ***sub-name@ctx-name*** [**detail**]

To display IPv4 filtering ACL information for one or more circuits, the syntax is:

show access-group ip-filter {**bvi** {***bvi-name*** | **id** ***bvi-id***} | **l2tp lns** ***lns-id*** | **mp** ***mp-id*** | ***slot*****/*****port*****:*****ch*****:*****sub*** [**:*****subsub***]} {**in** | **out**} [**all** | **conditions** | **counters** | **detail**]

show access-group ip-filter {**admin** | **interface** ***if-name*** | ***slot*****/*****port*****:*****ch*****:*****sub***} {**in** | **out**} [**all** | **counters** | **detail** | **log**]

To display IPv4 policy ACL information for one or more circuits to which a forward policy or quality of service (QoS) policy is attached, the syntax is:

show access-group {**forward** | **qos**} {**bvi** {***bvi-name*** | **id** ***bvi-id***} | **l2tp lns** ***lns-id*** | **mp** ***mp-id*** | ***slot*****/*****port*****:*****ch*****:*****sub*** [**:*****subsub***]} {**in** | **out**} [**all** | **conditions** | **counters** | **detail**]

To display policy ACL information for one or more circuits to which a Network Address Translation (NAT) policy is attached, the syntax is:

show access-group nat {**interface** *if-name* | **l2tp lns** *lns-id* | **mp** *mp-id* | *slot/port***:***ch***:***sub* [**:***subsub*] } {**in** | **out**} [**all** | **conditions** | **counters** | **detail**]

To display information about IPv4 ACLs applied to one or more reverse-path-forwarding (RPF)-enabled interfaces, the syntax is:

show access-group rpf [**interface** *if-name* **in** [**all** | **counters** | **detail**]]

To display information about administrative IPv4 ACLs that are applied to the current context, or about IPv4 ACLs or IP ACL access groups that are applied to specified ports, channels, circuits, or interfaces, or the Ethernet management port, the syntax is:

To display information about administrative IPv6 ACLs or access groups that are applied to the current context, or an interface, the syntax is:

show access-group ipv6 filter {**admin**] | **interface** *if-name*} {**in** | **out**} [**all** | **counters** | **detail**]

To display information about IPv6 filtering ACLs for circuits (including subscriber circuits), the syntax is:

show access-group ipv6 filter { **interface** *if-name* | **l2tp lns** *lns-id* | **l2vpn-cross-connect** [*l2vpn-prof-id*] | **lg** | **mip-fa** *mip-fa-id* | **mip-ha** *mip-ha-id* | **mp** *mp-id* | *slot/port***:***ch***:***sub* [**:***subsub*] } {**in** | **out**} [**all** | **conditions** | **counters** | **detail**]

To display policy ACL information for one or more circuits to which a forward policy or quality of service (QoS) policy is attached, the syntax is:

show access-group ipv6 {**forward** | **qos**} { **interface** *if-name* | **l2tp lns** *lns-id* | **l2vpn-cross-connect** [*l2vpn-prof-id*] | **lg** | **mip-fa** *mip-fa-id* | **mip-ha** *mip-ha-id* | **mp** *mp-id* | *slot/port***:***ch***:***sub* [**:***subsub*] } {**in** | **out**} [**all** | **conditions** | **counters** | **detail**]

1.76.1 Command Mode

All modes

1.76.2 Syntax Description

`all`	Optional. Displays all ACL information. In an ACL group, the information for the first ACL entry is more detailed than the subsequent entries.
`admin`	Displays administrative IP access group information.

bvi {id *bvi-id* | *bvi-name*}	Optional. Displays information about ACLs on BVI circuits. Not supported with IPv6 ACL groups.
conditions	Optional. Displays ACL conditions. Not supported for admin access groups.
counters	Optional. Displays ACL per-rule counters if counters are enabled in the access-list or access-group configuration.
detail	Optional. Displays detailed information, as listed in Table 20. Using the **detail** keyword allows you to check that rules exist for each ACL.
forward	Specifies ACLs applied to forward policies.
in	Displays ACL information for incoming traffic. For IP ACL access groups, ACLs appear in the same order that they appear in the access group.
interface *if-name*	Specifies the name of the interface for which information is to be displayed.
ip-filter	Specifies IPv4 ACL filtering is displayed.
ipv6 filter	Specifies IPv6 ACL filtering is displayed.
l2tp *l2tp-lns-id*	Specifies the Layer 2 Tunneling Protocol (L2TP) network server (LNS) circuit identifier. Limits information displayed to ACLs for the LNS circuit.
l2vpn *profile-name*	Specifies the Layer 2 Tunneling Protocol (L2TP) virtual private network (VPN) profile identifier. Limits information displayed to ACLs for the specified L2VPN.
l2vpn-cross-connect	Specifies the Layer 2 Tunneling Protocol (L2TP) virtual private network (VPN) profile identifier. Limits information displayed to ACLs for the cross-connect circuits.
sub-name@ctx-name	Subscriber name, followed by the @ symbol, followed by the context name.
lg	Enter the linkgroup of circuits to be shown.
mip-fa*mip-fa-id*	Optional. Displays Mobile IP Foreign Agent (FA) access group information.
mip-ha*mip-ha-id*	Optional. Displays Mobile IP Home Agent (HA) access group information.
mp *mp-id*	Optional. Merge point (MP) circuit identifier. Limits the output to the specified MP circuit.
nat	Specifies the policy ACLs applied to Network Address Translation (NAT) policies. Not supported with IPv6 ACLs.
out	Displays ACL information for outgoing traffic. Not available for RPF-enabled interfaces or for administrative ACLs.

qos	Specifies policy ACLs applied to quality of service (QoS) policies.
rpf	Specifies IP ACLs applied to an RPF-enabled interfaces.
log	Optional. Displays ACL deny log entries. Applicable for administrative ACLs only. Not supported for IPv6 access-groups or IPv6 admin access-groups.

1.76.3 Default

None

1.76.4 Usage Guidelines

Use the **show access-group** command to display information about configured administrative, IP filtering, and policy ACLs and the entities to which they are applied. Entities include one or more circuits, a forward, NAT, or QoS policy, or an interface, or a subscriber. This command displays information for both static and dynamic IP, policy ACLs, and configured access groups.

Run this command only if the traffic pattern is known and performance impact is not an issue.

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

The value for the *port* argument on the SmartEdge 100 router is one of the following:

- For a native port, it is 1 or 2.
- For a MIC port, it depends on the MIC and the MIC slot in which it is installed.

For an IPv6 subscriber, if you have enabled counters, use the **show access group ipv6 qos** ***slot/port*****:*****ch*****:*****sub*****:** [*subsub*] **in count** construct to view traffic flow. Enter the command twice, two to three minutes apart, to view incremented counters.

The ***slot/port*****:*****ch*****:*****sub*****:**[*subsub*] is the subscriber circuit where the counters were enabled.

Table 19 describes the fields displayed if you do not specify the **detail** keyword.

Table 19 Field Descriptions Without the detail Keyword

Field	Description
Circuit	Traffic card slot number, port number, and circuit identifier to which the ACL is applied.
ACL Name	ACL name. Up to ten names may exist.
Type	Policy ACL (forward, NAT, or QoS), IP ACL (regular, administrative, or RPF), or RADIUS guided (filter).
Interface Name	Name of the interface to which the ACL is applied.
Dir	Direction of traffic on the interface to which the ACL is applied.
Info	Flags: • C—Counters enabled for per-rule accounting. • L—Logging enabled. • M—ACL is configured in a different context. • S—Service accounting is enabled.
Rules	Number of rules or conditions configured in the ACL. For an IP ACL group, any ACL that shows zero (0) rules is not configured and is not active.

Table 20 describes the fields displayed if you specify the **`detail`** keyword.

Table 20 Field Descriptions for the detail Keyword

Field	Description
ACL type	Policy ACL (forward, NAT, or QoS), IP ACL (regular, administrative, or RPF), or RADIUS guided (filter).
ACL context	Context in which the ACL is created.
Circuit	Traffic card slot number, port number, and circuit identifier to which the ACL is applied. When an IP ACL has been applied to a layer 2 circuit through the **`ip access-group`** command, the circuit identifier field name is `Circuit [L2]`. In all other cases, the circuit identifier field name is simply `Circuit`.
Interface	Interface identifier to which the ACL is applied.
Direction	Direction of traffic on the interface to which the ACL is applied.

Table 20 Field Descriptions for the detail Keyword

Field	Description
ACL status	The following entries indicate the ACL status: • Applied—ACL is applied successfully. • Failed—ACL failed to download to the PPA. • In progress—ACL is being downloaded to the PPA. • No access-list—ACL is not yet configured. • No classes—Policy has no classes configured.
Count	Counter statistics on the number of hits per ACL rules: • No—Counter statistics are disabled. • Rules—Rule accounting is enabled. • Service—Service accounting is enabled.
Log	Optional. Displays ACL deny log entries. Applicable for administrative ACLs only. Not supported for IPv6 ACL groups. Information about the last 20 denied packets is saved in the system log.
IP Replacement	Replacement IP address in a dynamic IP or policy ACL rule. This field is displayed only if an ACL template is applied to the subscriber traffic.

For dynamic policy ACLs that use the vendor-specific attribute (VSA) 164 (Dynamic-Policy-Filter) provided by Ericsson AB, the system displays the Differentiated Services Code Point (DSCP) or type of service (ToS) setting in the rules, depending on the rule specified in the VSA 164 instance.

The system displays the DSCP option as `dscp` and the keyword for the DSCP setting in the rule, if one exists. Table 21 lists the DSCP keywords and their hexadecimal value substitutions; otherwise, a numeric value is displayed in decimal.

Note: Alternative keywords (**`precn`** and **`df`**) are not displayed; the primary keyword is displayed instead.

Table 21 Keywords for DSCP Values

Displayed Keyword	Hex Value	Definition
`af11`	0x0a	Assured Forwarding—Class 1/Drop Precedence 1
`af12`	0x0c	Assured Forwarding—Class 1/Drop Precedence 2

Table 21 Keywords for DSCP Values

Displayed Keyword	Hex Value	Definition
`af13`	0x0e	Assured Forwarding—Class 1/Drop Precedence 3
`af21`	0x12	Assured Forwarding—Class 2/Drop Precedence 1
`af22`	0x14	Assured Forwarding—Class 2/Drop Precedence 2
`af23`	0x16	Assured Forwarding—Class 2/Drop Precedence 3
`af31`	0x1a	Assured Forwarding—Class 3/Drop Precedence 1
`af32`	0x1c	Assured Forwarding—Class 3/Drop Precedence 2
`af33`	0x1e	Assured Forwarding—Class 3/Drop Precedence 3
`af41`	0x22	Assured Forwarding—Class 4/Drop Precedence 1
`af42`	0x24	Assured Forwarding—Class 4/Drop Precedence 2
`af43`	0x26	Assured Forwarding—Class 4/Drop Precedence 3
`cs0`	0x00	Class Selector 0
`cs1`	0x08	Class Selector 1
`cs2`	0x10	Class Selector 2
`cs3`	0x18	Class Selector 3
`cs4`	0x20	Class Selector 4
`cs5`	0x28	Class Selector 5
`cs6`	0x30	Class Selector 6
`cs7`	0x38	Class Selector 7
`ef`	0x2e	Expedited Forwarding
Nondisplayed Keywords	Hex Value	Definition
`df`	0x00	Default Forwarding (Alternative to `cs0`)
`prec1`	0x08	Precedence Selector 1 (Alternative to `cs1`)
`prec2`	0x10	Precedence Selector 2 (Alternative to `cs2`)
`prec3`	0x18	Precedence Selector 3 (Alternative to `cs3`)

Table 21 Keywords for DSCP Values

Displayed Keyword	Hex Value	Definition
`prec4`	0x20	Precedence Selector 4 (Alternative to `cs4`)
`prec5`	0x28	Precedence Selector 5 (Alternative to `cs5`)
`prec6`	0x30	Precedence Selector 6 (Alternative to `cs6`)
`prec7`	0x38	Precedence Selector 7 (Alternative to `cs7`)

For the ToS option, the system displays `tos`, the ToS group identifier, and the value. See Table 22 for a list of ToS group identifiers.

Table 22 ToS Mask Group Definitions

ToS Group	Bit Range	Decimal Value	Hex Value
Flags	1 to 4	30	0x1E
Precedence	5 to 7	224	0xE0
Combined	1 to 7	254	0xFE
DSCP	2 to 7	252	0xFC

Table 23 lists the identifiers that are displayed for the ToS values.

Table 23 Displayed Identifiers for ToS Values

Displayed Identifier	ToS Value	ToS Description
max-reliability	2	Maximum Reliable ToS
max-throughput	4	Maximum Throughput ToS
min-delay	8	Minimum Delay ToS
min-monetary-cost	1	Minimum Monetary Cost ToS
normal	0	Normal ToS

Table 24 lists the identifiers that are displayed for the ToS precedence values.

Table 24 Displayed Identifiers for ToS Precedence Values

Displayed Identifier	Precedence Value	Precedence Description
critical	5	Critical precedence
flash	3	Flash precedence
flash-override	4	Flash override precedence
immediate	2	Immediate precedence
internet	6	Internetwork control precedence

Table 24 Displayed Identifiers for ToS Precedence Values

Displayed Identifier	Precedence Value	Precedence Description
network	7	Network control precedence
priority	1	Priority precedence
routine	0	Routine precedence

Note: Hit counter and log information is displayed only if you have enabled these options using the **ip access-group** command in interface configuration mode or the **admin-access-group** command in context configuration mode.

Note: RPF enables the SmartEdge router to forward IP multicast traffic to the correct destination and prevents packet spoofing. The SmartEdge router looks up the source address of incoming traffic and verifies whether it has arrived on the interface that is on the reverse path back to the source. If so, the RPF check succeeds and the packet is forwarded. Otherwise the packet is dropped. The RPF check ensures that the IP multicast distribution tree has no loops and that no spoofed packets are forwarded.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

Table 25 Keywords and Arguments for the circuit-filter Argument

Keyword	Description
slot	Optional. Chassis slot number for a particular traffic card. If omitted, displays information about all circuits in the system.
port	Optional. Port number on the specified traffic card. If omitted, displays information about all circuits on the ports of the specified traffic card.
chan-num	Optional. Channel number for which circuits are displayed. If omitted, displays information for all channels on the specified port. The range of values depends on the type of port.

Table 25 Keywords and Arguments for the circuit-filter Argument

Keyword	Description
sub-chan-num	Optional. Subchannel number for which circuits are displayed. If omitted, displays information for all subchannels in the specified channel. The range of values depends on the type of port.
circuit-id	Optional. Circuit identifier, which is defined as: {**clips** *clips-id* | **dlci** *dlci* | **pppoe** *session-id* | **vlan** *vlan-id* | **vpi-vci** *vpi vci*} If omitted, displays information for all circuits on the specified traffic card, port, or channel.
clips *clips-id*	Clientless IP service selection (CLIPS) circuit on a port, channel, 802.1Q PVC, or ATM PVC. The range of values is 1 to 262,144. If the CLIPS circuit is on an 802.1Q or ATM PVC, you specify this construct in addition to the circuit identifier for the 802.1Q or ATM PVC.
dlci *dlci*	Data-link connection identifier (DLCI) for the Frame Relay permanent virtual circuit (PVC). The range of values is 16 to 991.
pppoe *session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session identifier. The range of values is 1 to 65,535.
vlan *vlan-id*	Virtual LAN (VLAN) tag value for an 802.1Q tunnel or PVC. The *vlan-id* argument is one of the following constructs: • **pvc-vlan-id**—VLAN tag value of a PVC that is not within an 802.1Q tunnel. If you specify the VLAN tag value for an 802.1Q tunnel, the output includes subscriber information for all the PVCs within the tunnel. • **tunl-vlan-id**—VLAN tag value of a tunnel. • **tunl-vlan-id:pvc-vlan-id**—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel. The range of values for any VLAN tag value is 1 to 4,095.
vpi-vci *vpi vci*	Virtual path identifier (VPI) and virtual circuit identifier (VCI) for an ATM PVC. The range of values is 0 to 255 and 1 to 65,535, respectively. By convention, VCI 1 to 31 are reserved for system use.

1.76.5 Examples

The following example displays all configured ACLs in the local context:

```
[local]Redback#show access-group

  (Enabled Info: C-counters; L-logging; S-service; M-ACL in diff context)

Circuit                ACL Name          Type      Dir Info Rules
3/4 vlan-id 3 clips 4  ADF FI_00000009  Filter    In  CL       6
3/4 vlan-id 3 clips 4  qos1             QoS       In  C S     21
3/4 vlan-id 3 clips 4  DPF QI_0000000A  QoS       In  C S      2
```

The following example displays counts for one IPv4 filtering ACL rule processing incoming traffic on interface, `if1`:

```
[local]Redback#show access-group ip-filter interface if1 in count
Circuit lg id 25 lg1, slot 5, IPv4 access-list, img 0x80000001 list1, in, 1 rules

Hit Count:          0  No Match (Default)
Hit Count:          0  seq 55 permit ip any any
```

The following example displays detailed information about an ACL when per-rule accounting is enabled:

```
[local]Redback#show access-group forward 3/7 in detail


Forwarding ACL : fwd1

ACL context    : local

Circuit        : 3/7

Direction      : In          ACL status  : No classes

Count          : Rules       Log         : N/A
```

The following example displays detailed information about an ACL when service accounting is enabled:

```
[local]Redback#show access-group forward 3/7 in detail


Forwarding ACL : fwd1
ACL context    : local
Circuit        : 3/7
Direction      : In          ACL status  : No classes
Count          : Service     Log         : N/A
```

The following example displays information about the policy ACL and ACL conditions applied to the forward policy attached to incoming traffic on port **1** of the traffic card installed in slot **3:**

```
[local]Redback#show access-group forward 3/1 in conditions
  --- circuit 3/1, slot 3, access group redirect_acl, in, rules ---

  seq 10 permit tcp any any eq www class redir0 condition 101 [redir2]
  seq 20 permit tcp any any eq 81 class redir1
  seq 30 permit tcp any any eq 82 class redir2
```

The following example displays RPF ACL hit counts for incoming traffic on the **e1** interface:

```
[local]Redback#show access-group rpf interface e1 in counters

 --- Circuit 3/1 slot 3 access group tc in counters ---

Hit Count:         0  No Match (Default)
Hit Count:         0  seq 10 deny ip host 1.1.1.1 host 2.2.2.1
Hit Count:         0  seq 20 permit ip host 1.1.1.2 host 2.2.2.2
Hit Count:         0  seq 30 deny ip host 1.1.1.3 host 2.2.2.3
Hit Count:         0  seq 40 permit ip host 1.1.1.4 host 2.2.2.4
Hit Count:         0  seq 50 deny ip host 1.1.1.5 host 2.2.2.5
Hit Count:         0  seq 60 permit ip host 1.1.1.6 host 2.2.2.6
Hit Count:         0  seq 70 deny ip host 1.1.1.7 host 2.2.2.7
```

The following example displays **all** dynamic policy ACL information for incoming traffic on **clips** circuit **1** with a **forward** policy attached to it:

```
[local]Redback#show access-group forward 2/1 clips 1 in all


Forwarding ACL : DPF PI_00000003

ACL context    : local

Circuit        : 2/1 clips 1

Direction      : In          ACL status  : Applied

Count          : No          Log         : N/A

Number of rules: 5

Circuit 2/1 clips 1, slot 2, access group DPF PI_00000003, in, rules:

seq 10 permit ip host 11.1.0.51 any tos max-throughput class c1

seq 20 permit ip host 11.1.0.51 any precedence immediate class c1

seq 30 permit ip host 11.1.0.51 any precedence immediate tos max-throughput class c1

seq 40 permit ip host 11.1.0.51 any tos 6 class c1

seq 50 permit ip host 11.1.0.51 any dscp eq af41 class c1
```

The following example displays output for IPv6 admin ACLs:

```
[local]Redback#show access-group ipv6 filter admin in
  (Enabled Info: C-counters; L-logging; S-service; M-ACL in diff context)
Circuit                 ACL Name       Prot Type   Ifc Name      Dir Info Rules
                        list6            v6 Filter admin         In  C        6
```

The following example displays IPv6 ACL hit counts for outgoing traffic on the **C6** interface:

```
[local]Redback#show access-group ipv6 filter interface C6 out count
Circuit 5/2, slot 5, IPv6 access-list list6, out, 7 rules
Hit Count:         0  No Match (Default)
Hit Count:         0  seq 10 permit ipv6 any any traffic-class eq ef
Hit Count:         0  seq 20 permit tcp any any invalid-tcp-flags
Hit Count:         0  seq 30 permit tcp any any setup
Hit Count:         0  seq 40 permit ipv6 any any fragments
Hit Count:         0  seq 50 permit tcp any any setup fragments
Hit Count:         0  seq 60 permit ipv6 any any traffic-class eq af11 fragments
Hit Count:       130  seq 100 permit ipv6 any any
```

The following example displays output with the ***all*** keyword:

```
[local]Redback#show access-group ipv6 filter admin in all

IPv6 Fltr ACL   : list6
ACL context     : local
Circuit         :
Interface       : admin-access-group
Direction       : In          ACL status  : Applied
Count           : Rules       Log         : No


Admin IPv6 access-list list6, in, 6 rules

Hit Count:         0  No Match (Default)
Hit Count:         0  seq 10 deny tcp 21::/64 eq 1024
Hit Count:         0  seq 12 deny tcp 22:1:1::2/128 any traffic-class eq df
Hit Count:         0  seq 15 deny fragment any any
Hit Count:         0  seq 20 deny udp any any range 80 81
Hit Count:         0  seq 30 deny esp any any
Hit Count:         0  seq 900 permit ipv6 any any
```

1.77 show access-line

show access-line [{**neighbor** ***ip-addr***[**:*remote-port***] | **agent-circuit-id** ***string***}]

1.77.1 Purpose

Displays digital subscriber line (DSL) information for one or more DSLs.

1.77.2 Command Mode

all modes

1.77.3 Syntax Description

neighbor	Optional. Displays DSL information for the DSLs attached to this Access Node Control Protocol (ANCP) neighbor peer.
ip-addr	IP address for the ANCP neighbor peer for one or more DSL lines.
remote-port	Optional. Transmission Control Protocol (TCP) port number for this ANCP neighbor peer. The range of values is 1 to 65,535. If not specified, displays DSL information for all neighbors with the specified IP address.

`agent-circuit-id`	Optional. Displays DSL information for the DSL with this circuit agent ID only. This includes the current maximum session-limit, the number of sessions that are UP, and the total number of sessions in progress (authenticating).
`string`	Circuit agent ID. A text string, with up to 63 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces.

1.77.4 Default

When entered without any optional syntax, the **`show access-line`** command displays DSL information for all ANCP neighbor peers.

1.77.5 Usage Guidelines

Use the **`show access-line`** command to display DSL information for one or more DSLs. This information includes the parameters learned from the DSL attribute extension Type, Length, Value (TLV) in the General Switch Management Protocol (GSMP) Port Up message for the DSL. The fields that this command displays for the ANCP neighbor peer (the DSL access multiplexer [DSLAM]) to which the DSL is attached include:

- Name (system ID) of the ANCP router
- Remote agent ID specified for the subscriber on this DSL

DSL fields are preceded by the source of the data:

- ANCP—Identifies data from the ANCP neighbor peer (the DSLAM).
- DSLF (DSL Forum)—Identifies data from a Point-to-Point Protocol (PPP) over Ethernet (PPPoE) tag or Dynamic Host Control Protocol (DHCP) tag in option 82.

Table 26 lists the types of DSL data and the values that this command can display; fields that are not transmitted to the SmartEdge router are not displayed.

Table 26 DSL Data for the show access-line Command

Type of Data	Values
DSL line state	• IDLE (DSL is down) • SHOWTIME (DSL is active) • SILENT (DSL is down)

Table 26 DSL Data for the show access-line Command

Type of Data	Values
DSL type (transmission system)	• Asymmetric DSL (ADSL)1, ADSL2, ADSL2+ • Unknown • Very-high data rate DSL (VDSL)1, VDSL2, SDSL
DSL data rates	• Actual data rates upstream (inbound to the SmartEdge router) and downstream (outbound from the SmartEdge router) in Kbps[1] • Minimum and maximum data rates upstream and downstream in Kbps • Attainable data rates upstream and downstream in Kbps • Minimum low power data rates upstream and downstream in Kbps • Actual and maximum interleaving delay upstream and downstream in msec
Data link protocol	• Asynchronous Transfer Mode (ATM) adaptation layer 5 (AAL5) • Ethernet
Data link encapsulation 1	• Single-tagged Ethernet • Untagged Ethernet
Data link encapsulation 2	• Ethernet over AAL5 LLC with Frame Check Sequence (FCS) • Ethernet over AAL5 LLC without FCS • Ethernet over AAL5 with FCS • Ethernet over AAL5 without FCS • IP over ATM (IPoA) LLC • IPoA NULL • PPP over ATM (PPPoA) logical link control (LLC) • PPPoA NULL

(1) If you have configured the access-line rate command in subscriber configuration mode and the actual data rate has been applied to the subscriber circuit, this command displays these fields with "(applied)" after the rate.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.77.6 Examples

The following example displays DSL information for ANCP neighbor peer **abc-2.1:**

```
[local]Redback#show access-line agent-circuit-id abc-2.1

"abc-2.1"
        Agent Remote ID "xyz-2.1"
        Neighbor ID 30.100.1.20:3871
        DSLF Transmission System                           ADSL1
        DSLF Line State                                    SHOWTIME
        DSLF Actual Data Rate Upstream (kbps)              256 (applied)
        DSLF Actual Data Rate Downstream (kbps)            512 (applied)
        DSLF Minimum Data Rate Upstream (kbps)             32
        DSLF Minimum Data Rate Downstream (kbps)           32
        DSLF Attainable Data Rate Upstream (kbps)          1280
        DSLF Attainable Data Rate Downstream (kbps)        10784
        DSLF Maximum Data Rate Upstream (kbps)             256
        DSLF Maximum Data Rate Downstream (kbps)           512
        DSLF Minimum low power Data Rate Upstream (kbps)   32
        DSLF Minimum low power Data Rate Downstream (kbps) 32
        DSLF Maximum Interleaving Delay Upstream (mSec)    20
        DSLF Actual Interleaving Delay Upstream (mSec)     16
        DSLF Maximum Interleaving Delay Downstream (mSec)  20
        DSLF Actual Interleaving Delay Downstream (mSec)   16
        ANCP Access-Loop-Encapsulation
                Data Link = ATM AAL5
                Encps 1   = NA
                Encps 2   = PPPoA LLC
        PPPoA/oE IWF session
```

1.78 show administrators

show administrators [**active** [*admin-name*]] [**sftp-session** | **ssh-telnet-session**]

1.78.1 Purpose

Displays all administrator sessions on a system.

1.78.2 Command Mode

all modes

1.78.3 Syntax Description

active	Optional. Restricts the display to active administrators in the current context.
admin-name	Optional. Name of a particular administrator.
sftp-session	Optional. For SFTP sessions, displays the IP address and session type.
ssh-telnet-session	Optional. For Telnet and SSH sessions, displays the IP address and session type.

1.78.4 Default

Displays all administrator sessions.

1.78.5 Usage Guidelines

Use the **show administrators** command to display all administrator sessions on a system. Use the **active** keyword to limit the display to active sessions. With the **active** keyword, you can also use the ***admin-name*** argument to specify the sessions corresponding to a particular administrator.

In the display, the asterisk (*) character denotes the administrator session in which this command was entered.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct before the **show** command to view output for the specified context without entering that context. For more information about the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.78.6 Examples

The following example displays output from the **show administrators** command when used without optional constructs:

```
[local]Redback#show administrators

  TTY    START TIME                REMOTE HOST             ADMINISTRATOR
-----------------------------------------------------------------------
  ttyp0  Mon Jun 27 14:42:53 2005 nosuchhost.redback.com  test@local
* ttyp1  Mon Jun 27 09:12:31 2005 dhcp-xx.redback.com     last@local
  ttyp2  Mon Jun 27 11:15:43 2005 dhcp-yy.redback.com     test@local
```

The following example displays output from the **show administrators** command when a specific administrator name is specified:

```
[local]Redback#show administrators active test

  TTY    START TIME                REMOTE HOST             ADMINISTRATOR
-----------------------------------------------------------------------
* ttyp0  Mon Jun 27 05:34:38 2005 155.53.6.209            test@local
  ttyp2  Mon Jun 27 11:15:43 2005 dhcp-yy.redback.com     test@local
```

1.79 show alias

show alias [{**inherit** | ***mode***}]

1.79.1 Purpose

Displays a list of command aliases defined on the system.

1.79.2 Command Mode

all modes

1.79.3 Syntax Description

inherit	Optional. Displays the aliases in all modes.
mode	Optional. Command mode in which the alias applies.

1.79.4 Default

Displays all aliases defined on the system.

1.79.5 Usage Guidelines

Use the **show alias** command to display a list of the command aliases defined on the system.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.79.6 Examples

The following example displays output from the **show alias** command:

```
[local]Redback#show alias

Alias          Mode              Command

spc            all               show port counters

users          exec              show users show clock
```

1.80 show ancp

show ancp

1.80.1 Purpose

Displays Access Node Control Protocol (ANCP) global information.

1.80.2 Command Mode

all modes

1.80.3 Syntax Description

This command has no keywords or arguments.

1.80.4 Default

None

1.80.5 Usage Guidelines

Use the **show ancp** command to display ANCP global information.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.80.6 Examples

The following example displays global ANCP information:

```
[local]Redback#show ancp


ANCP (GSMP) global info

Flags: T - Topology discovery, L - Line Configuration,

       M - Multicast transaction, O - OAM

-------------------------------------------------------------

versions             : 3.1

capability           : TO (master)

system id            : default (ca:ef:18:07:29:09)

listening port       : default (6068)

keepalive (retry)    : 10 secs retry 3

neighbor connection  : 0

cfg neighbor profile : 1

cfg neighbor intf    : 1
```

1.81 show ancp neighbor

show ancp neighbor [{**ip-address** ***ip-addr***[**:*remote-port***] | **profile** ***prof-name***}]

1.81.1 Purpose

Displays Access Node Control Protocol (ANCP) session information for one or more ANCP neighbor peers or for an ANCP profile.

1.81.2 Command Mode

All modes

1.81.3 Syntax Description

ip-address ***ip-addr***	Optional. Displays information for the ANCP neighbor peer with the specified IP address.
remote-port	Optional. TCP port number. The range of values is 1 to 65,535.
profile ***prof-name***	Optional. Displays information for the ANCP neighbor peers that use this ANCP neighbor profile.

1.81.4 Default

When entered without any optional syntax, the **show ancp neighbor** command displays a summary of ANCP session information for all ANCP neighbor peers.

1.81.5 Usage Guidelines

Use the **show ancp neighbor** command to display ANCP session information for one or more ANCP neighbor peers. ANCP session information includes Transmission Control Protocol (TCP) and General Switch Management Protocol (GSMP) information. Summary information includes a single line for each ANCP session and a line that displays the total number of ANCP sessions and the total number of ANCP neighbor peers.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.81.6 Examples

The following example displays information for all ANCP neighbor peers:

```
[local]Redback#show ancp neighbor

ANCP (GSMP) neighbor info
Flags: T - Topology discovery, L - Line Configuration,
       M - Multicast transaction, O - OAM
-------------------------------------------------------------
capability           : T (client)
master port          : 6068
master sender name   : 00:30:88:00:04:b7
ip address:port      : 10.4.1.2:7001
peer id              : 33:33:33:44:44:44
profile              : default
incoming interface   : default (0x00000000)
keepalive            : 10 secs, retry 3
instance id          : 00:00:2b/00:00:a2
access port/part id  : 1/201
adjacency state      : ESTABLISHED
uptime               : 7 secs
```

1.82 show ancp neighbor statistics

show ancp neighbor [**ip-address** *ip-addr*[**:***remote-port*]] **statistics**

1.82.1 Purpose

Displays Access Node Control Protocol (ANCP) neighbor statistics.

1.82.2 Command Mode

All modes

1.82.3 Syntax Description

ip-address ***ip-addr***	Optional. Displays statistics for the ANCP neighbor peer with the specified IP address.
remote-port	Optional. TCP port number. The range of values is 1 to 65,535.

1.82.4 Default

When entered without any optional syntax, the **show ancp neighbor statistics** command displays statistics for all ANCP neighbor peers.

1.82.5 Usage Guidelines

Use the **show ancp neighbor statistics** command to display ANCP neighbor statistics for one or more ANCP neighbor peers.

Use the **ip-address** ***ip-addr*** construct to display statistics for a single ANCP neighbor peer.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.82.6 Examples

The following example displays ANCP neighbor statistics for a single ANCP neighbor peer:

```
[local]Redback#show ancp neighbor ip-address 10.4.1.2: 4001 statistics

ANCP (GSMP) neighbor packet statistics
-------------------------------------------------------------
ip address:port      : 10.4.1.2:4001
packet sent--------------------------------------------------
syn                 0 port up              0
syn ack             1 port down            0
ack                13 port new             0
rstack              0 port dead            0
adj update          0 port mgmt            0
packet receive-----------------------------------------------
syn                 1 port up            100
syn ack             0 port down            0
ack                 1 port new             0
rstack              0 port dead            0
adj update          0 port mgmt            0
packet receive version error---------------------------------
syn                 0 port up              0
syn ack             0 port down            0
ack                 0 port new             0
rstack              0 port dead            0
adj update          0 port mgmt            0
packet receive partition id error----------------------------
syn                 0 port up              0
syn ack             0 port down            0
ack                 0 port new             0
rstack              0 port dead            0
adj update          0 port mgmt            0
packet receive master bit error------------------------------
syn                 0 syn ack              0
ack                 0 rstack               0
packet receive event not establish error---------------------
port up             0 port down            0
port new            0 port dead            0
```

1.83 show aps

show aps group [*aps-group-name*] [**detail**]

1.83.1 Purpose

Displays Automatic Protection Switching (APS) information and statistics for one or more APS groups in the system.

1.83.2 Command Mode

all modes

1.83.3 Syntax Description

group	Displays group information.
aps-group-name	Optional. APS group for which information is to be displayed.
detail	Optional. Provides detailed APS information.

1.83.4 Default

Displays information for all APS groups.

1.83.5 Usage Guidelines

Use the **show aps** command to display information and statistics for one or more APS groups in the system. Use the optional **aps-group-name** argument to limit the display to information for a specific APS group. Table 27 lists the fields displayed by this command and their possible values.

Table 27 Field Descriptions for the show aps Command

Field	Description
Protection Group	*aps-group-name*—Configured name of the APS group.
ID	System-assigned group identifier.
Type	Line card type.
Description	Description of line card.

Table 28 lists the additional fields displayed by the **detail** keyword.

Table 28 Field Descriptions for the show aps Command with the detail Keyword

Field	Description
Interface Bound	*`if-name`*—Interface to which the working port is bound. Unbound—Working port is not yet bound to any interface. N/A—For ATM APS groups; port bindings are not supported for ATM ports.
Card Type	Line card type.
Architecture	Protection type (1+1).
Direction	Bidirectional.
Switch Mode	• Nonrevertive—If the failed working port is restored to service, it becomes the protect port. • Revertive—If the failed working port is restored to service, it reverts, after the wait-to-restore (WTR) interval has expired, to the working port.
Extra Traffic	No—Protection port cannot be used to carry extra traffic in 1+1 architecture.
CHPR	Current highest-priority request (CHPR): • No Request • Exercise • Wait to Restore • Manual Switch • Auto Switch • Forced Switch • Lockout Protection
Switch Trigger Reason	Reason for the last switch. See Table 29.
Switch Failed Reason	Why the last switch failed: • No Reason—Switch did not fail. • Local Bridge or Switch—The near end failed to bridge or switch its traffic. • Remote Bridge or Switch—The far end failed to bridge or switch its traffic.
Maintenance Mode	IS—In Service. Protection group is currently active. OOS—Out of Service. Protection group is currently inactive.
Wtr	Configured value for the WTR interval (1 to 60 minutes).

Table 28 Field Descriptions for the show aps Command with the detail Keyword

Field	Description
Wtr Status	Active—Port is in the WTR state. Inactive—Port is not in the WTR state.
Lockout Status Manual Switch Status Forced Switch Status Auto Switch Status	Status of each type of switch: • Completed—Switch request has been completed. • Failed—Switch request has failed. • Idle—No switch request of this type is posted. • Pending—Switch request has been initiated. • Requested—Switch request has been posted.
Tx Traffic	Active—This port is transmitting traffic. Standby—This port is not transmitting traffic.
Rx Traffic	Active—This port is receiving traffic. Standby—This port is not receiving traffic.
Tx K1 Byte Rx K1 Byte Tx K2 Byte Rx K2 Byte	Values of the received and transmitted K1 and K2 bytes at the local end in an APS configuration.
Port Alarms	Types of alarms that generate an alarm message.
ATM/POS Port Alarms(1)	Types of alarms that are generated with alarm-report-only setting.

(1) The port alarm groups are different under the different port type and SONET/SDH mappings.

Table 29 lists the reasons a switch can be triggered.

Table 29 Reasons for a Switch Request

Reason	Description
No Reason	No known switch request posted.
User Request	Switch request initiated by an administrator (lockout, force, or manual).
Signal Degraded	Signal bit error rate (BER) exceeded configured threshold (SD-BER) for this port.
EBER	Excessive BER detected.
Signal Failed	The BER exceeded the configured threshold (SF-BER) for this port. The port is shutdown, or the port or traffic card has failed.

Table 29 Reasons for a Switch Request

Reason	Description
AIS	Alarm indication signal received.
Equipment Forced Failed	The port is in an OOS state. The **shutdown** command in port configuration mode entered by administrator.
Equipment Missing	Traffic card not installed.
Equipment Mismatched	Port types not identical.
Equipment Failed	Port or traffic card failed.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.83.6 Examples

The following example displays information for all APS groups:

```
[local]Redback#show aps group
```

The following example displays detailed information for the APS group **pos:**

```
[local]Redback#show aps group atm1 detail
```

```
Protection Group: atm1, ID: 1, Type: am
Description     :

[local]Redback#show aps group atm1 detail
Protection Group: atm1, ID: 1, Type: atm
Description     :
---------------------------------------------------------------------------
Interface Bound: N/A
Card Type      : oc3                         Architecture    : 1+1
Direction      : Unidirectional              Switch Mode     : Non-Revertive
Extra Traffic  : No                          CHPR            : Auto Switch
Switch Trigger Reason    : AIS
Switch Failed Reason     : No Reason
Maintenance Mode         : IS

Working Port: 6/1 Information
---------------------------------
Wtr                   : 5              Wtr Status            : Inactive
Lockout Status        : Idle           Manual Switch Status  : Idle
Forced Switch Status  : Idle           Auto Switch Status    : Completed
Tx Traffic            : Standby        Rx Traffic            : Standby
Tx K1 Byte            : 0x00           Rx K1 Byte            : 0xff
Tx K2 Byte            : 0x00           Rx K2 Byte            : 0xff
Port Alarms
=================================================
Report Only Alarms
  Path Alarms (report only): Path remote defect indication (RDI-P)
Active Alarms              : Line alarm indication signal (AIS-L)
                           : Port auto switch completed
STS Path Alarms            : NONE

Protect Port: 6/2 Information
---------------------------------
Wtr                   : 5              Wtr Status            : Inactive
Lockout Status        : Idle           Manual Switch Status  : Idle
Forced Switch Status  : Idle           Auto Switch Status    : Idle
Tx Traffic            : Active         Rx Traffic            : Active
Tx K1 Byte            : 0xc1           Rx K1 Byte            : 0xc1
Tx K2 Byte            : 0x14           Rx K2 Byte            : 0x14
Port Alarms
=================================================
Report Only Alarms
  Path Alarms (report only): Path remote defect indication (RDI-P)
Active Alarms              : NONE
STS Path Alarms            : NONE
```

The following example shows how to create the APS group **atm1** and display information for the group:

```
[local]Redback#show aps group
```

The following example displays the APS group **atm1** and the protect group information:

```
Protection Group: atm1, ID: 1, Type: atm
---------------------------------------------------------------------------
Interface Bound: UnBound
Card Type      : oc3                  Architecture   : 1+1
Direction      : Bidirectional        Switch Mode    : Revertive
Extra Traffic  : No                   CHPR           : Auto Switch
Switch Trigger Reason   : Signal Failed
Switch Failed Reason    : No Reason
Maintenance Mode        : IS
Working Port: 3/1 Information
--------------------------------
Wtr                   : 15             Wtr Status            : Inactive
Lockout Status        : Idle           Manual Switch Status  : Idle
Forced Switch Status  : Idle           Auto Switch Status    : Pending
Tx Traffic            : Active         Rx Traffic            : Active
Tx K1 Byte            : 0x00           Rx K1 Byte            : 0x00
Tx K2 Byte            : 0x00           Rx K2 Byte            : 0x00        Port Alarms
================================
Active Alarms         : SFP
STS Path Alarms       : NONE
VT Path Alarms        : NONE

Protect Port: 3/2 Information
---------------------------------
Wtr                   : 15             Wtr Status            : Inactive
Lockout Status        : Idle           Manual Switch Status  : Idle
Forced Switch Status  : Idle           Auto Switch Status    : Completed
Tx Traffic            : Standby        Rx Traffic            : Standby
Tx K1 Byte            : 0x00           Rx K1 Byte            : 0x00
Tx K2 Byte            : 0x05           Rx K2 Byte            : 0x05
Port Alarms
=================================
Active Alarms         : NONE
STS Path Alarms       : NONE
VT Path Alarms        : NONE
```

1.84 show arp-cache

`show arp-cache` [*`ip-addr`*] [**`detail`**]

1.84.1 Purpose

Displays Address Resolution Protocol (ARP) information for the controller card.

1.84.2 Command Mode

all modes

1.84.3 Syntax Description

`ip-addr`	Optional. IP address of a specific host.
`detail`	Optional. Displays detailed information for the specified IP address.

1.84.4 Default

None

1.84.5 Usage Guidelines

Use the **show arp-cache** command to display ARP information for the controller card.

Use the ***ip-addr*** argument to display ARP information for the specified IP address.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context *ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context *ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.84.6 Examples

The following example displays ARP information for the controller card:

```
[local]Redback#show arp-cache


Total number of arp entries in cache: 4
  Resolved entry   : 4
  Incomplete entry : 0
Host                 Hardware address     Ttl     Type   Circuit
3.2.13.3             00:30:88:00:12:86    -       ARPA   13/3
4.2.13.4             00:30:88:00:12:87    -       ARPA   13/4
192.168.11.1         00:30:88:00:12:8e    -       ARPA   13/11
192.168.12.1         00:30:88:00:12:8f    -       ARPA   13/12
```

1.85 show arp-cache all

show arp-cache all

1.85.1 Purpose

Displays Address Resolution Protocol (ARP) information for both the Berkeley Standard Distribution (BSD) and the controller card for the current context.

1.85.2 Command Mode

all modes

1.85.3 Syntax Description

This command has no keywords or arguments.

1.85.4 Default

None

1.85.5 Usage Guidelines

Use the **show arp-cache all** command to display ARP information for both the BSD and the controller card for the current context.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.85.6 Examples

The following example displays all ARP table information:

```
[local]Redback#show arp-cache all
```

```
Total number of arp entries in cache: 2
  Resolved entry    : 2
  Incomplete entry : 0

Host                Hardware address    Ttl     Type   Circuit
40.1.1.1            00:30:88:00:77:00   -       ARPA   12/5
40.1.1.2            00:30:88:00:76:02   3585    ARPA   12/5
Showing ARP entries on Cross-connect RP:
Host                Hardware address    Ttl     Type
10.13.49.100        00:d0:b7:5a:f3:5f   1181    ARPA
10.13.49.254        00:10:67:00:20:a4   1200    ARPA
```

1.86 show arp-cache all-context

show arp-cache all-context

1.86.1 Purpose

Displays Address Resolution Protocol (ARP) information for both the Berkeley Standard Distribution (BSD) and the controller card for all contexts.

1.86.2 Command Mode

all modes

1.86.3 Syntax Description

This command has no keywords or arguments.

1.86.4 Default

None

1.86.5 Usage Guidelines

Use the **`show arp-cache all-context`** command to display ARP information for both the BSD and the controller card for all contexts.

Note: By default, most **`show`** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see ***`context`***.

Note: By appending a space followed by the pipe (I) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.86.6 Examples

The following example displays all ARP information for all contexts:

```
[local]Redback#show arp-cache all-context
```

```
Context   :local                          Context id  : 0x40080001
Total number of arp entries in cache: 2
  Resolved entry   : 2
  Incomplete entry : 0

Host              Hardware address    Ttl    Type  Circuit
40.1.1.1          00:30:88:00:77:00   -      ARPA  12/5
40.1.1.2          00:30:88:00:76:02   3549   ARPA  12/5
Context   :faq                            Context id  : 0x40080081
-------------------------------------------------------------------
Total number of arp entries in cache: 0


Context   :2                              Context id  : 0x40080082
-------------------------------------------------------------------
Total number of arp entries in cache: 2
  Resolved entry   : 2
  Incomplete entry : 0

Host              Hardware address    Ttl    Type  Circuit
40.1.1.1          00:30:88:00:77:00   3549   ARPA  12/7
40.1.1.2          00:30:88:00:76:02   -      ARPA  12/7
```

1.87 show arp-cache interworking

show arp-cache interworking ***slot/port*** [**vlan-id** ***vlan-id***]

1.87.1 Purpose

Displays Address Resolution Protocol (ARP) information for cross-connections between Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) and 802.1Q PVCs.

1.87.2 Command Mode

all modes

1.87.3 Syntax Description

slot	Optional. Chassis slot number. If omitted, displays information about all circuits in the system.
port	Optional. Traffic card port number. If omitted, displays information about all circuits on all ports of the specified traffic card.
vlan-id *vlan-id*	Optional. Virtual LAN (VLAN) tag value for the 802.1Q PVC. The range of values is 1 to 4,095. If omitted, displays the ARP cache for the entire circuit.

1.87.4 Default

None

1.87.5 Usage Guidelines

Use the **show arp-cache interworking** command to display ARP information for cross-connections between ATM PVCs and 802.1Q PVCs.

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Note: The command used to configure interworking cross-connections is the **xc** command in global configuration mode; for more information, see *Configuring Cross-Connections*.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, ssee *context*.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.87.6 Examples

The following example displays ARP information for cross-connections between ATM PVCs and 802.1Q PVCs:

```
[local]Redback#show arp interworking

Routed Host       VLAN Host         VLAN Hardware address
10.0.0.1          10.0.0.1          00:10:67:00:4d:65
20.0.0.1          20.0.0.1          00:10:67:00:4d:66

[local]Redback#show arp interworking detail

-------------------------------------------------------------
Displaying information for ARP Interworking circuit 12/1 vlan-id 32
Int representation       : 12/1:1023:63/1/2/38 Circuit State      : UP

Local Hardware address    : 00:30:88:00:76:fc
Remote Hardware address   : 00:10:67:00:4d:65
VLAN  IP address          : 10.0.0.1            Routed IP address   : 10.0.0.2



-------------------------------------------------------------
Displaying information for ARP Interworking circuit 12/1 vlan-id 33
Int representation        : 12/1:1023:63/1/2/39 Circuit State       : UP

Local Hardware address    : 00:30:88:00:76:fc
Remote Hardware address   : 00:10:67:00:4d:66
VLAN  IP address          : 20.0.0.1            Routed IP address   : 20.0.0.2
```

The following example displays ARP information for VLAN ID **32:**

```
[local]Redback#show arp interworking 12/1 vlan-id 32

-------------------------------------------------------------
Displaying information for ARP Interworking circuit 12/1 vlan-id 32
Int representation        : 12/1:1023:63/1/2/38 Circuit State       : UP

Local Hardware address    : 00:30:88:00:76:fc
Remote Hardware address   : 00:10:67:00:4d:65
VLAN  IP address          : 10.0.0.1            Routed IP address   : 10.0.0.2
```

1.88 show arp-cache statistics

`show arp-cache statistics` [**`xcrp`** | **`all`**]

1.88.1 Purpose

Displays Address Resolution Protocol (ARP) statistics.

1.88.2 Command Mode

all modes

1.88.3 Syntax Description

`xcrp`	Optional. Displays statistics for the controller card only.
`all`	Optional. Displays statistics for both the Berkeley Standard Distribution (BSD) and the controller card.

1.88.4 Default

None

1.88.5 Usage Guidelines

Use the **`show arp-cache statistics`** command to display ARP statistics.

Note: By default, most **`show`** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see ***`context`***.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.88.6 Examples

The following example displays ARP statistics:

```
[local]Redback#show arp-cache statistics


Display ARP traffic statistics:

    Rcvd: 3 requests, 0 replies, 0 other, 0 bad

    Sent: 3 requests, 0 replies

    InvArp: 0 request-rcvd, 0 reply-sent
```

1.89 show arp-cache summary

show arp-cache summary

1.89.1 Purpose

Displays summary information about the Address Resolution Protocol (ARP) table.

1.89.2 Command Mode

all modes

1.89.3 Syntax Description

This command has no keywords or arguments.

1.89.4 Default

None

1.89.5 Usage Guidelines

Use the **show arp-cache summary** command to display summary information about the ARP table.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see *context*.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.89.6 Examples

The following example displays summary information about the ARP table:

```
[local]Redback#show arp-cache summary


Showing ARP entries on Cross-connect RP:

Host               Hardware address     Ttl     Type

10.13.49.100       00:d0:b7:5a:f3:5f    1198    ARPA

10.13.49.254       00:10:67:00:20:a4    1199    ARPA
```

1.90 show arp-cache xcrp

show arp-cache xcrp [*ip-addr*]

1.90.1 Purpose

Displays Address Resolution Protocol (ARP) information for the controller card.

1.90.2 Command Mode

all modes

1.90.3 Syntax Description

ip-addr	Optional. Specific host IP address to be displayed.

1.90.4 Default

None

1.90.5 Usage Guidelines

Use the **show arp-cache xcrp** command to display ARP information for the controller card.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.90.6 Examples

The following example displays ARP information for the controller card:

```
[local]Redback#show arp-cache xcrp


Showing ARP entries on Cross-connect RP:
Host                Hardware address    Ttl    Type
10.13.49.100        00:d0:b7:5a:f3:5f   1198   ARPA
10.13.49.254        00:10:67:00:20:a4   1199   ARPA
```

1.91 show as-path-list

show as-path-list [*apl-name* | **first-match** *as-path-string acl-name* | **summary**]

1.91.1 Purpose

Displays information about configured Border Gateway Protocol (BGP) autonomous system (AS) path lists.

1.91.2 Command Mode

all modes

1.91.3 Syntax Description

apl-name	Optional. AS path list name. Required when using the **first-match** keyword construct.
first-match	Optional. Searches for the first match specified by the ***as-path-string*** argument. Searches for the line in the AS path list specified by the ***acl-name*** argument.
as-path-string	Text to search for in the specified AS path. Required when using the **first-match** keyword.
acl-name	Name of access control list that is searched for in the AS path list. Required when using the **first-match** keyword.
summary	Optional. Displays AS path summary information.

1.91.4 Default

Displays information about BGP AS path lists.

1.91.5 Usage Guidelines

Use the **show as-path-list** command to display information about configured BGP AS path lists.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.91.6 Examples

The following example displays all AS path lists configured for the **local** context:

```
[local]Redback#show as-path-list

as-path-list AS2686:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 20 hour(s) ago
   seq 10 permit _2686$  (hits: 6,  cache hits: 3)
as-path-list AS7777:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 20 hour(s) ago
   seq 10 permit _7777$  (hits: 765529,  cache hits: 765511)
as-path-list deny_AS-5619$:
 count: 2, sequences: 10 - 20, client count: 1
 modified: 2 day(s), 20 hour(s) ago
   seq 10 deny _5619$  (hits: 4,  cache hits: 2)
   seq 20 permit .*  (hits: 62867,  cache hits: 34976)
total as-path lists: 3
```

The following example displays summary information for AS path lists configured in the **local** context:

```
[local]Redback#show as-path-list summary
```

```
as-path-list AS2686:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 20 hour(s) ago
as-path-list AS7777:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 20 hour(s) ago
as-path-list deny_AS-5619$:
 count: 2, sequences: 10 - 20, client count: 1
 modified: 2 day(s), 20 hour(s) ago
total as-path lists: 3
```

1.92 show atm counters

show atm counters [all] [profile *prof-name*] [*slot*/*port* [vp vpi *vpi* summary | vpi *vpi* [vci *vci* [through *end-vci*]]]] [details [errors] | no-counter | port-stats | queues | summary [errors]]

1.92.1 Purpose

Displays cell and segmentation and reassembly (SAR) packet-level counters for configured Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.92.2 Command Mode

all modes

1.92.3 Syntax Description

all	Optional. Displays traffic counters for all configured PVCs. This option is available only in the local context.
profile ***prof-name***	Optional. Name of an ATM profile.
slot	Optional. Chassis slot number of an ATM traffic card with counters to be displayed.

port	Optional. Port number of an ATM port with counters to be displayed; see Table 30.
vp	Optional. Virtual path tunnel statistics counter containing traffic information for an ATM PVC channel direct from an SAR client.
start-vpi	Optional. Starting virtual path identifier (VPI). The range of values is 0 to 255.
through *end-vpi*	Optional. Last VPI in the range.
start-vci	Optional. Starting virtual circuit identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use.
end-vci	Optional. Last VCI in the range.
details	Optional. Displays more details for each PVC.
errors	Optional. Displays counters only for PVCs that have nonzero error counters.
no-counter	Optional. Displays only PVCs that do not have counters enabled.
port-stats	Optional. Displays operations, administration, and management (OAM) circuit creation on demand (CCOD) counters. This option is available only if you enter the *slot* and *port* arguments.
queues	Optional. Displays virtual channel (VC) tunnel statistics for each class-of-service (CoS) queue.
summary	Optional. Displays only a summary of bound and unbound PVCs.

1.92.4 Default

Displays cell and SAR packet-level counters for all configured ATM PVCs that are bound in the current context.

1.92.5 Usage Guidelines

Use the **show atm counters** command to display cell and SAR packet-level counters for configured ATM PVCs. PVC traffic statistics for each PVC are not kept by the system by default. Enter the **counters** command in ATM profile configuration mode to enable statistics collection.

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 30 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

Table 30 Port Ranges for ATM Traffic Cards

Traffic Card Type	Physical Ports	Low-Density Version	Low-Density Ports
8-port ATM OC-3c/STM-1c	8	No	–
2-port ATM OC-12c/STM-4c	2	No	–

Note: The value for the ***port*** argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

Consider the following guidelines when using the **show atm counters** command:

- In the local context, specify the **all** keyword to show all configured ATM PVCs, including both bound PVCs (any context) and unbound PVCs. In any other context, the display includes only PVCs that are bound within the current context.
- If you specify a profile name, the output displays counters for PVCs configured with that profile only.
- If you specify the ***slot*** and ***port*** arguments, the output displays PVCs configured on that slot and port only.
- If you specify the **vp vpi** ***vpi*** construct, the output displays PVC statistics counts. If a PVC counter is reset, the **vp vpi** ***vpi*** construct returns the number of PVC counts since the last counter reset and all other PVCs in the same VP tunnel. If a PVC is deleted from a VP tunnel, the **vp vpi** ***vpi*** construct returns only the counts of existing PVCs on the VP tunnel.
- If you specify the VPI number, the output displays PVCs configured with that VPI only. If you also specify a VCI, the output displays that PVC only. If you specify the **through** keyword, the output displays the counters for the specified range of VCIs.
- If you specify the **details** keyword, the display includes detailed output for each specified PVC; otherwise, it displays two lines of output for each PVC.
- If you specify the **errors** keyword, the output displays only the counters for the PVCs with errors.
- If you specify the **no-counters** keyword, the output displays only the PVCs that do not have counters enabled.
- If you specify the **port-stats** keyword, the output displays only the ATM SAR port-level counters. This option is available only if ***slot*** and ***port*** arguments are configured.
- If you specify the **summary** keyword, the output displays a summary only; it does not include counters for each PVC. Otherwise, the output displays cells sent and packets dropped as the aggregate of all the queues for a VC tunnel.

- Use the **show atm counters queue** command to obtain accurate per-queue statistics for ATM PVCs.

- Use the optional keywords in different combinations to show specific PVCs. For example, use the **profile** and **detail** keywords to display detailed counter information for PVCs that you have configured with a specific profile in the current context. This command displays no output if no PVCs match the conditions that you specify with the keywords.

- A channel number is always 1 for ATM OC ports. If you specify the **vp vpi** keywords together, the output displays VP statistics counters. The VP statistics counter is the sum of PVC statistics counters in the same VP tunnel. If a PVC counter is reset, the **vp vpi** keywords return the PVC counters since the last counter reset and the counters for all other PVCs in the same VP tunnel. If a PVC is deleted from a VP tunnel, the **vp vpi** keywords return only the counters of remaining PVCs on the VP tunnel.

- The per-queue transmit byte (octet) counters currently include the padding bytes in the ATM adaptation layer type 5 (AAL5) common part convergence sublayer-protocol data unit (CPCS-PDU); therefore, the values reported by these counters are higher than the actual values.

By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.92.6 Examples

The following example shows how to display counters for all ATM PVCs that have counters configured:

```
[local]Redback#show atm counters
```

```
current time: Fri Mar 19 18:26:27 2005

                       Pkts/Cells Pkts/Cells Xmt Pkts Rcv Pkts
  Port:Channel VPI  VCI Received   Sent       Dropped  Dropped
   1/2 :1      10  123 0          0          0        0
                       0          0
   1/2 :1      10  124 0          0          0        0
                       0          0
   1/2 :1      10  125 0          0          0        0
                       0          0
   1/2 :1      10  126 0          0          0        0
                       0          0
   1/2 :1      10  127 0          0          0        0
                       0          0
   1/2 :1      10  128 0          0          0        0
                       0          0
   1/2 :1      10  129 0          0          0        0
                       0          0
   1/2 :1      10  130 0          0          0        0
                       0          0
pvc with counters: 13    pvc without counters: 0
  Cells Rcvd:                     0 Cells Sent:                      0
  Packets Rcvd:                   0 Packets Sent:                    0
  Rcv Packets Dropped:            0 Xmt Packets Dropped:             0
  OAM Cells Rcvd:                 0 OAM Cells Sent:                195
  OAM AIS Rcvd:                   0 OAM AIS Sent:                    0
  OAM RDI Rcvd:                   0 OAM RDI Sent:                    0
                                    OAM Cells Dropped:               0
```

The following example shows how to display a summary of counters:

```
[local]Redback#show atm counters summary
```

```
current time: Fri Mar 19 18:26:27 2005

pvc with counters: 1       pvc without counters: 0
  Cells Rcvd:                 322605 Cells Sent:                 322656
  Packets Rcvd:                30973 Packets Sent:                30975
  Rcv Packets Dropped:             0 Xmt Packets Dropped:             0
  OAM Cells Rcvd:                  0 OAM Cells Sent:                  0
  OAM AIS Rcvd:                    0 OAM AIS Sent:                    0
  OAM RDI Rcvd:                    0 OAM RDI Sent:                    0
                                     OAM Cells Dropped:               0
```

The following example shows how to display counters for a specific ATM PVC:

```
[local]Redback#show atm counters 2/2 vpi 10 vci 10
```

```
current time: Fri Mar 19 18:26:27 2005

Port:Chan:  2/2  :1     VPI: 10  VCI: 10     Profile: ubr
Status: Up
Bound to: atm2_1@local
First Created: Wed Oct 15 20:24:51 2003
Modified Last: Wed Oct 15 20:24:51 2003
Last Cleared: never
  Cells Rcvd:                     4258147 Cells Sent:             4258208
  Packets Rcvd:                    408785 Packets Sent:            408788
  OAM Cells Rcvd:                       0 OAM Cells Sent:               0
  OAM AIS Rcvd:                         0 OAM AIS Sent:                 0
  OAM RDI Rcvd:                         0 OAM RDI Sent:                 0
                                          OAM Cells Dropped:            0
  Rcvd Pkts Dropped:                    0 Xmt Pkts Dropped:             0
  WRED Hi Threshold Dropped:            0 WRED Probability Dropped:     0
```

The following example shows how to display the counters, including the queues for all VC tunnels (ATM PVC), on a specific port:

```
[local]Redback#show atm counters 2/2 queues
```

```
current time: Fri Mar 19 18:26:27 2005
                          Pkts         Probability  HiThreshold  Resource
Port:Channel VPI VCI    Q Sent         Drops (Pkts) Drops (Pkts) Drops (Pkts)
 2/2 :1      10  10     1 367927       0            0            0
 2/2 :1      10  10     2 7433593      0            0            0
```

The following example displays ATM PVC counters for this VP tunnel using the **show atm counters** ***slot/port*** **vp vpi** ***vpi*** command:

```
[local]Redback#show atm counters 3/1 vp vpi 101
current time: Thu Aug 20 04:16:53 2009
                   Pkts/Cells   Pkts/Cells   Xmt Pkts     Rcv Pkts
  Port:Channel VPI Received     Sent         Dropped      Dropped
   3/1         101 20           20           0            0
                   40           40
pvc with counters: 0       pvc without counters: 0
  Cells Rcvd:                      40 Cells Sent:                         40
  Packets Rcvd:                    20 Packets Sent:                       20
  OAM Cells Rcvd:                  20 OAM Cells Sent:                     20
  AIS OAM Cells Rcvd:               0 AIS OAM Cells Sent:                  0
  RDI OAM Cells Rcvd:               0 RDI OAM Cells Sent:                  0
                                      OAM Cells Dropped:                   0
  Rcvd Pkts Dropped:                0 Xmt Pkts Dropped:           0
```

1.93 show atm profile

show atm profile [***prof-name*** | **detail**]

1.93.1 Purpose

Displays information about one or all Asynchronous Transfer Mode (ATM) profiles configured in the current context.

1.93.2 Command Mode

all modes

1.93.3 Syntax Description

prof-name	Optional. Name of an existing ATM profile.
detail	Optional. Displays detailed information for all ATM profiles configured in the current context.

1.93.4 Default

When used without any options, displays summary information in tabular form for all ATM profiles configured in the current context.

1.93.5 Usage Guidelines

Use the **show atm profile** command to display information about one or all ATM profiles configured in the current context. Table 31 lists the fields that are displayed if the **detail** keyword or a profile name is not specified.

Table 31 Field Descriptions for the show atm profile Command Without Options

Field	Description
Name	Name specified by the **atm profile** command; an asterisk (*) character indicates a static profile.
Shaping Mode	Traffic class specified by the **shaping** command.
Counters	Statistics collection as specified by the **counters** command.
CLPBIT	Status as specified by the **clpbit** command: On, Off, or QoS to atm.
MCR	Traffic class parameter as specified by the **shaping** command.
PCR	Traffic class parameter as specified by the **shaping** command.
CDVT	Traffic class parameter as specified by the **shaping** command.
SCR	Traffic class parameter as specified by the **shaping** command.
BT	Traffic class parameter as specified by the **shaping** command.

Table 32 lists the fields that are displayed when the **detail** keyword or a profile name is specified; fields are not displayed for options that are not configured.

Table 32 Field Descriptions for the show atm profile Command with Either Option

Field	Description
Name	Name specified by the **atm profile** command; static profiles are indicated with STATIC.
Description	Profile description specified by the **description** command.
Class of Service	Traffic class including values for the traffic class arguments, specified by the **shaping** command.(1)
Counters	Statistics collection as specified by the **counters** command.
CLPBIT	Status as specified by the **clpbit** command: On, Off, or QoS to atm.

Table 32 Field Descriptions for the show atm profile Command with Either Option

Field	Description
Congestion Avoidance	EPD or WRED as specified by the **epd** or **red** keyword for the **congestion** command, followed by: • EPD Parameters—Values specified if the **epd** option is specified for the **congestion** command. • WRED Parameters—Default values or values specified if the **red** option is specified for the **congestion** command.
OAM Parameters	Status and, if enabled, values specified by the **oam xc**, **oam fault-monitoring**, or **oam manage** command: • Cross-Connect OAM. • Fault Monitoring. • OAM Managed.

(1) When displaying a profile that specifies the CBR traffic class, the value configured for the cdvt argument in the shaping command is shown in the CDV field.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.93.6 Examples

The following example shows how to display detailed information about the ATM profile **atm-pro:**

```
[local]Redback#show atm profile atm-pro
```

```
Name                          : atm-pro
Description                   :
Class of Service              : UBR
Counters                      : None
CLPBIT                        : Off
Congestion Avoidance          : WRED
  WRED Parameters:
   Min Threshold              : 5
   Max Threshold              : 15
   Probability                : 129
   Weight                     : 9
OAM Parameters:
   Cross-Connect OAM Cells    : Disabled
   Fault Monitoring           : Disabled
   OAM Managed                : Disabled
```

The following example shows how to display detailed information about the ATM profile **atm-epd:**

```
[local]Redback#show atm profile atm-epd

Name                          : atm-epd
Description                   :
Class of Service              : UBR
Counters                      : None
CLPBIT                        : Off
Congestion Avoidance          : EPD
  EPD Parameters:
   Min Threshold              : 8      ATM-OC3-2port & ATM-OC12-1port cards ONLY
   Max Threshold              : 987
OAM Parameters:
   Cross-Connect OAM Cells    : Disabled
   Fault Monitoring           : Disabled
   OAM Managed                : Disabled
```

1.94 show atm pvc

show atm pvc [**aps standby**] [***slot*/*port*** [[**vpi**] ***vpi*** [[**vci**] ***start-vci*** [**through** ***end-vci***]]]] [**all**] [**dynamic**] [**profile** ***prof-name***] [**summary** | **up** | **down**]

1.94.1 Purpose

Displays static Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.94.2 Command Mode

All modes

1.94.3 Syntax Description

aps standby	Optional. Displays the PVCs stored in the APS standby ports.
slot	Optional. Chassis slot number of an ATM traffic card with PVCs to be displayed. The range of values depends on the chassis in which the card is installed; see Table 33.
port	Required if you enter the ***slot*** argument. Port number with PVCs to be displayed. The range of values depends on the type of traffic card; see Table 34.

start-vpi	Optional. Starting virtual path identifier (VPI). The range of values is 0 to 255.
through *end-vpi*	Optional. Last VPI in the range.
start-vci	Optional. Starting virtual circuit identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use.
end-vci	Optional. Last VCI in the range.
all	Optional. Displays PVCs in all contexts.
dynamic	Optional. Displays only the subscriber-based PVCs that are authenticated by the RADIUS and that have been dynamically modified by RADIUS during the active session to use a different profile.
profile *prof-name*	Optional. Name of an ATM profile.
summary	Optional. Displays only summary information.
up	Optional. Displays only operable PVCs.
down	Optional. Displays only inoperable PVCs.

1.94.4 Default

Displays all static ATM PVCs that are bound within the current context.

1.94.5 Usage Guidelines

Use the **show atm pvc** command to display static ATM PVCs.

Table 33 lists the values for the *slot* argument for the SmartEdge 800 and SmartEdge 400 chassis; in the table, the IR abbreviation is used for Intermediate Reach.

Table 33 Slot Ranges for ATM Traffic Cards

	slot Argument Range	
Traffic Card Type	**SmartEdge 400 Router**	**SmartEdge 800 Router**
8-port ATM OC-3c/STM-1c 2-port ATM OC-12c/STM-4c	1 to 4	1 to 6 and 9 to 14

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 34 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

Table 34 Port Ranges for ATM Traffic Cards

Traffic Card Type	Physical Ports	Low-Density Version	Low-Density Ports
8-port ATM OC-3c/STM-1c	8	No	–
2-port ATM OC-12c/STM-4c	2	No	–

Note: The value for the *port* argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

Use the **all** keyword to display all existing ATM PVCs, including both bound PVCs (any context) and unbound PVCs. If not specified, the output includes only PVCs within the current context.

Use the **aps standby** keyword to display the PVCs stored in the APS standby ports.

Use the **dynamic** keyword to display only those subscriber-based ATM PVCs that have been authenticated by RADIUS and that have been dynamically modified by RADIUS during the active session to use a different profile. The **dynamic** keyword works with any of the other keywords and constructs.

If you specify a profile name by using the **profile** keyword, the output displays only PVCs configured with that profile.

If you specify the *slot* and *port* arguments, the output displays only PVCs created on that slot and port.

If you specify the **vpi** *vpi* construct, the output displays only PVCs created with that VPI. If you also specify the **vci** *vci* construct, the output displays only that PVC. If you use the **through** *end-vci* construct, the output includes the specified range of VCIs.

If you use the **summary** keyword, the output includes only a summary; it does not display individual PVC data.

Use the **up** keyword to display only operable PVCs; use the **down** keyword to display only inoperable PVCs.

Table 35 lists the fields that can be displayed by this command for a specific PVC; fields are not displayed if not appropriate.

Table 35 Field Descriptions for the show atm pvc Command

Field	Description
Port:Channel	Slot and port specified by this command; the channel is always 1 for ATM OC ports.
VPI: VCI:	VPI and VCI specified by this command.
Profile	Profile name specified by the **atm pvc** command.

Table 35 Field Descriptions for the show atm pvc Command

Field	Description
Description	Description specified by the **description** command.
Status	Up or Down.
Counters	Statistics collection as specified by the **counters** command for the profile. The counters column (Ctrs) can indicate: • None—No counters were specified in the profile. • L2—The **counters l2** command (layer 2) was entered for the profile.
Encapsulation	Encapsulation as specified by the **atm pvc** command.
Bound to	Interface to which bound; no binding if no binding has been created.
Binding Cfg	Command used to create the binding; not displayed if no binding has been created.
QoS - outbound ATMWFQ policy	• None if no policy was specified. • Name of QoS policy.
Circuit Range	PVC created as part of a range (using the **explicit** keyword): • no—Circuit is created as individual circuit. • yes—CIrcuit is part of a range of circuits.
CCOD	Type of ATM PVC; displayed only if the PVC is one of a range of PVCs: • no—Range of static PVCs. • yes—Range of on-demand PVCs.
Authorize Type	• AAA. • Local.
First Created	Date PVC was created.
Status Change	Date PVC status was last changed.
OAM Cross-Connect	Status of PVC and **oam xc** command: • Disabled—Command is not enabled. • Enabled but not cross-connected—Command is enabled in the ATM profile but this PVC is not cross-connected. • Enabled—Command is enabled in the ATM profile and PVC is cross-connected; includes Connection type is Connection Point and values specified by the command.

Table 35 Field Descriptions for the show atm pvc Command

Field	Description
OAM Managed	Status of PVC and **oam managed** command: • Disabled—Command is not enabled. • Enabled using Fault Monitoring (AIS/RDI) and Heartbeat. • Enabled using Fault Monitoring (AIS/RDI) and Auto-Loopback—Status of auto-loopback: Success.
OAM Fault Monitoring	Source of fault management: • Disabled—OAM fault monitoring (**oam fault-monitor** command) is disabled. • Enabled—OAM fault monitoring is enabled. • OAM Managed—OAM management (**oam manage** command) is enabled. • OAM XC—OAM management is enabled and PVC is cross-connected.
AIS or RDI	AIS or RDI state if fault monitoring is enabled by one of the **oam** commands: • Set—AIS or RDI alarm is present. • Clear—No AIS or RDI alarm is present.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.94.6 Examples

The following example shows how to display a specific PVC that is not cross-connected:

```
[local]Redback#show atm pvc 6/1 vpi 1 vci 101
```

```
Port:Channel  6/1 :1       VPI: 1    VCI: 101    Profile: oam
Description: circuit to Tokyo
Status:   Up  Counters: None  Encapsulation:  multi1483
Bound to: no binding
Circuit Range: no
First Created: Sun Jan 12 13:12:26 2003
Status Change: Sun Jan 12 13:12:26 2003
OAM Cross Connect: Disabled
OAM Managed: Disabled
OAM Fault Management: Disabled
```

The following example shows how to display all configured PVCs:

```
[local]Redback#show atm pvc all

Traffic
Port:Channel VPI VCI    Profile    State Ctrs Encaps              Binding
 6/1 :1      1   32     1.ubr      Down  L2   route1483             ---
 6/1 :1      1   39     1.vbrrt    Down  L2   multi1483             ---
 6/1 :1      32  1      pf-atm1    Down  L2   ipoe                  ---
 6/1 :1      32  2      pf-atm1    Down  L2   multi1483             ---
 6/2 :1      1   32     1.ubr      Down  L2   route1483             ---
 6/2 :1      1   33     1.vbrrt    Down  L2   bridge1483            ---
 6/2 :1      1   34     1.ubr      Down  L2   ipoe                  ---
 6/2 :1      1   40     1.ubr      Down  L2   route1483             ---
pvcs up: 0  pvcs down: 8        total pvcs: 8
```

The following examples displays two subscriber-based PVCs that have had their profiles changed dynamically by RADIUS. In the first example, the configured traffic profiles are shown; in the second example, the dynamically assigned traffic profiles are shown:

```
[local]Redback#show atm pvc
```

```
Traffic
Port:Channel VPI VCI   Profile    State Ctrs Encaps           Binding
 3/1 :1      10  10    atm-gold   Up    None ppp              ---
 3/1 :1      10  11    atm-gold   Up    None ppp              ---
pvcs up: 2      pvcs down: 0    total pvcs: 2

[local]Redback#show atm pvc dynamic

Traffic
Port:Channel VPI VCI   Profile    State Ctrs Encaps           Binding
 3/1 :1      10  10    atm-silv   Up    None ppp              ---
 3/1 :1      10  11    atm-silv   Up    None ppp              ---
pvcs up: 2      pvcs down: 0    total pvcs: 2
```

The following example shows how to display all PVCs on standby APS port **5/1:**

```
[local]Redback#show atm pvc 5/1

Traffic
Port:Channel VPI VCI   Profile    State   Ctrs Encaps           Binding
5/1 :1       0   32    ubr        S/Down  L2   ppp              ---
5/1 :1       0   33    ubr        S/Down  L2   ppp              ---
pvcs up: 0 pvcs down: 2 total pvcs: 2
```

1.95 show atm pvc on-demand

show atm pvc on-demand [**aps standby**] [***slot/port*** [[**vpi**] ***vpi*** [[**vci**] ***start-vci*** [**through** ***end-vci***]]]] [**active** | **all** | **dormant** | **summary**]

1.95.1 Purpose

Displays on-demand Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.95.2 Command Mode

All modes

1.95.3 Syntax Description

aps standby	Optional. Displays the on-demand PVCs stored in the APS standby ports.
slot	Optional. Chassis slot number of an ATM traffic card with PVCs to be displayed. The range of values depends on the chassis in which the card is installed; see Table 36.
port	Required if you enter the *slot* argument. Port number with PVCs to be displayed. The range of values depends on the type of traffic card; see Table 37.
start-vpi	Optional. Starting virtual path identifier (VPI). The range of values is 0 to 255.
through *end-vpi*	Optional. Last VPI in the range.
start-vci	Optional. Starting virtual circuit identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use.
end-vci	Optional. Last VCI in the range.
active	Optional. Displays only on-demand PVCs with active subscriber sessions.
all	Optional. Displays PVCs in all contexts.
dormant	Optional. Displays only on-demand PVCs that are in listening mode.
summary	Optional. Displays only summary information.

1.95.4 Default

Displays all on-demand ATM PVCs in the current context.

1.95.5 Usage Guidelines

Use the **show atm pvc on-demand** command to display on-demand ATM PVCs.

Table 36 lists the values for the *slot* argument for each type of SmartEdge chassis; in the table, the IR abbreviation is used for Intermediate Reach.

Table 36 Slot Ranges for ATM Traffic Cards

	slot **Argument Range**	
Traffic Card Type	**SmartEdge 400 Router**	**SmartEdge 800 Router**
8-port ATM OC-3c/STM-1c 2-port ATM OC-12c/STM-4c	1 to 4	1 to 6 and 9 to 14

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 37 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

Table 37 Port Ranges for ATM Traffic Cards

Traffic Card Type	**Physical Ports**	**Low-Density Version**	**Low-Density Ports**
8-port ATM OC-3c/STM-1c	8	No	–
2-port ATM OC-12c/STM-4c	2	No	–

Note: The value for the *port* argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

Use the **all** keyword to display all on-demand ATM PVCs, including both bound PVCs (any context) and unbound PVCs. If not specified, the output includes only PVCs within the current context.

If you specify the *slot* and *port* arguments, the output displays only PVCs created on that slot and port. The PVCs may be listed by range order and may not necessarily be in ascending order.

Use the **aps standby** keyword to display the on-demand PVCs stored in the APS standby ports.

If you specify the **vpi** *vpi* construct, the output displays only PVCs created with that VPI. If you also specify the **vci** *vci-start* construct, the output displays only that PVC. If you use the **through** *end-vci* construct, the output includes the specified range of VCIs.

If you use the **summary** keyword, the output includes only the summary line that is displayed at the end of the output; it does not display individual PVC data.

Use the **active** keyword to display active PVCs; use the **dormant** keyword to display PVCs that are in listening mode.

Table 38 lists the fields that can be displayed by the **show atm pvc on-demand** command.

Table 38 Field Descriptions for the show atm pvc on-demand Command

Field	Description
Port:Channel	Slot and port specified by this command; the channel is always 1 for ATM OC ports.
VPI	VPI in the specified range.
VCI	VCI in the specified range.
VC HANDLE	Internal circuit identifier.
State	Up or Down status.
Encaps	Configured encapsulation for this PVC. on-demand—PVC is dormant.
Binding	Interface to which bound. no binding—**`bind`** command has not been entered.
Mode	• active—Circuit is active with traffic. • dormant—Circuit is in listening mode. • idle-down—Circuit has no active subscriber sessions; the idle-down watchdog timer is running. • wait—Dormant circuit has not yet been created.
active	Number of PVCs that are configured and subscribers are currently using.
idle	Number of PVCs that are configured but no subscriber is using.
idle-down	Number of PVCs that are configured and for which the idle-down watchdog timer has started.
static	Number of static PVCs that have been created in this range.
wait	Number of dormant PVCs that are in the process of being created or deleted in this range.
dormant	Number of dormant PVCs that have been created on the SARC and PPA in this range.
total	Number of PVCs in this range.

Note: By default, most **`show`** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see ***`context`***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.95.6 Examples

The following example shows how to display data for all on-demand PVCs:

```
[local]Redback#show atm pvc on-demand

active: 0 idle: 0 idle-down: 0 wait-cfg: 1
static: 0 wait: 0 dormant: 0
total: 1
```

The following example shows how to display the state of an on-demand PVC when the configuration is not yet completed (the circuit has not been bound):

```
[local]Redback#show atm pvc on-demand

Port:Channel VPI VCI   VC HANDLE  State Encaps        Binding          Mode
1/1 :1       1   1     ---        Down  on-demand     no binding       dormant
4/1 :1       1   1     ???        Down  on-demand     no binding       limbo
10/1 :1      1   1     ---        Up    on-demand     no binding       dormant
10/2 :1      1   1     ???        Down  on-demand     no binding       wait cfg
active:  0    idle: 0 idle-down: 0 wait-cfg: 1
static:  0    wait: 0 dormant:   2 limbo:    1
total:   4
```

The following example shows how to display the state of an on-demand PVC when the configuration is complete and the circuits are active:

```
[local]Redback#show atm pvc on-demand 3/1

Port:Channel VPI VCI   VC HANDLE  State Encaps        Binding          Mode
3/1 :1       10  32    1000       Up multi            test_intf@local  active
3/1 :1       10  32    1000       Up pppoe            ---              active
```

The following example shows how to display the on-demand PVCs configured on the APS standby ports:

```
[local]Redback#show atm pvc on-demand aps standby


Port:Channel VPI VCI   VC HANDLE  State   Encaps       Binding          Mode
5/2 :1       20  32    ???        S/Down  on-demand    no binding       wait cfg
5/2 :1       20  33    ???        S/Down  on-demand    no binding       wait cfg
5/4 :1       20  32    ???        S/Down  on-demand    no binding       wait cfg
5/4 :1       20  33    ???        S/Down  on-demand    no binding       wait cfg
active: 0 idle: 0 idle-down: 0 wait-cfg: 4
static: 0 wait: 0 dormant: 0 limbo: 0
total: 4
```

The following example shows how to display the VCI status for a specific VPI:

```
[local]Redback#show atm pvc on-demand 11/1 vpi 2
```

```
Port:Channel VPI VCI   VC HANDLE  State Encaps        Binding          Mode
11/1 :1        2  501  ---        Up    on-demand     no binding       dormant
11/1 :1        2  101  ---        Up    on-demand     no binding       dormant
active:  0 idle: 0 idle-down: 0
static:  0 wait: 0 dormant: 2
total:   2
```

1.96 show atm pvc on-demand range

show atm pvc on-demand range [*slot*/*port* [*start-vpi*:*start-vci* **through** *end-vpi*:*end-vci*]]

1.96.1 Purpose

Displays range statistics for on-demand Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

1.96.2 Command Mode

All modes

1.96.3 Syntax Description

slot	Optional. If not specified, statistics for all ATM PVC circuits are displayed. If specified, this argument is the chassis slot number of an ATM traffic card with PVCs to be displayed. The range of values depends on the chassis in which the card is installed; see Table 39.
port	Required if you enter the *slot* argument. If not specified, statistics for all ATM PVC circuits are displayed. If specified, this argument is the port number with PVCs to be displayed. The range of values depends on the type of traffic card; see Table 40.
start-vpi	Optional. Starting virtual path identifier (VPI) for the range that is configured for the port. The range of values is 0 to 255.
start-vci	Optional. Starting virtual circuit identifier (VCI) for the range that is configured for the port. The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use.
through *end-vpi*	Optional. Last VPI in the range that is configured for the port.
end-vci	Optional. Last VCI in the range that is configured for the port.

1.96.4 Default

None

1.96.5 Usage Guidelines

Use the **show atm pvc on-demand range** command to display range statistics for the specified ATM PVC range. If you want to display the statistics for a given port, you must specify the entire range of on-demand PVCs that are configured for the port as the *start-vpi*:*start-vci* **through** *end-vpi*:*end-vci* construct. If you specify a subset of a configured range, no statistics are displayed. Use the **show configuration** command in port configuration mode to find out what the configured range of on-demand PVCs is for the port.

Table 39 lists the values for the *slot* argument for each type of SmartEdge router; in the table, the IR abbreviation is used for Intermediate Reach.

Table 39 Slot Ranges for ATM Traffic Cards

	slot Argument Range	
Traffic Card Type	**SmartEdge 400 Router**	**SmartEdge 800 Router**
8-port ATM OC-3c/STM-1c 2-port ATM OC-12c/STM-4c	1 to 4	1 to 6 and 9 to 14

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 40 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

Table 40 Port Ranges for ATM Traffic Cards

Traffic Card Type	Physical Ports	Low-Density Version	Low-Density Ports
8-port ATM OC-3c/STM-1c	8	No	–
2-port ATM OC-12c/STM-4c	2	No	–

Note: The value for the *port* argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

In the local context, use the **all** keyword to display range statistics for all existing ATM PVCs on the specified port. The **all** keyword is available only in the local context. In any other context, the output includes range statistics for only the PVCs that are bound within the current context.

Table 41 lists the fields that can be displayed by this command; fields are not displayed if not appropriate.

Table 41 Field Descriptions for the show atm pvc on-demand range Command

Field	Description
Port:Channel	Slot and port specified by this command; the channel is always 1 for ATM OC ports.
VPI: VCI:	Starting VPI and VCI in the range.
through VPI: VCI	Last VPI and VCI in the range.
Attempts	Number of attempts to create an on-demand circuit with the specified VPI and VCI.
Success	Number of successful attempts to create an on-demand circuit with the specified VPI and VCI.
Failure	Number of failed attempts to create an on-demand circuit with the specified VPI and VCI.
Authorize Type	Authorization for on-demand circuit: • AAA—Authorization provided by authentication, authorization, and accounting (AAA). • Local—Local authorization.
Idle Down Configured	For on-demand circuits: • Yes—Number of seconds configured by the **`idle-down`** command in ATM PVC configuration mode. • No—Idle down not configured.
Range Created on SARC/PPA	For on-demand circuits: • Yes—Range has been created. • No—Configuration is in process or the full configuration is not complete.
Failure Statistics	See Table 42.

Table 42 lists the field definitions for the statistics displayed by this command.

Table 42 Statistics Field Descriptions

Field	Description
No shaping profile	Shaping profile was not found in the AAA attribute list.
Shaping profile not found	Specified shaping profile was not configured in the SmartEdge router.
No encap	No encapsulation type was specified in the AAA attribute list.
Non ATM encap	Specified encapsulation type is not supported by ATM.
Unsupported ATM encap	Specified ATM encapsulation type is not supported for on-demand PVCs.

Table 42 Statistics Field Descriptions

Field	Description
No binding	Binding was not found in the AAA attribute list.
No binding applied on range	The On-demand range does not have a binding configured.
Bad bind type for encap	Binding found in the AAA attribute list does not match the encapsulation type.
No authen protocols	Bind type was “authentication”, but no authentication protocols were specified.
No sub name	Bind type was “subscriber”, but no subscriber name was specified.
No auto-sub name	Bind type was “auto-subscriber”, but no auto-subscriber name was specified.
PVC exists in RCM	Attempted to create an on-demand PVC, but the Router Configuration Manager (RCM) indicates it already exists.
Create PVC failure in RCM	RCM could not create the PVC.
Delete PVC failure in RCM	RCM could not delete the PVC.
CCOD range not found in RCM	Attempted to create an on-demand PVC, but the on-demand range was not found in RCM.
Internal Error	An unexpected internal error has occurred.
RCM endpoint down	Failed to send create PVC because the RCM endpoint was down.
AAA endpoint down	Failed to send authorize message to AAA because the AAA endpoint was down.
RCM restarted	Failed to create the PVC because the RCM was restarted.
AAA restarted	Failed to authorize the PVC with RADIUS because AAA was restarted.
AAA method failure	AAA returned a method failure. RADIUS server might not be configured.
AAA authorization failure	AAA failed to find the PVC configuration in RADIUS.
SARC open error	Failed to open the segmentation and reassembly controller (SARC) channel for dormant on-demand entry.
SARC close error	Failed to close the SARC channel for dormant on-demand entry.
No Memory	Failed to allocate memory for the AAA authorization or RCM circuit creation message.
TLV failure	TLV library has produced an unexpected error.
System call error	A system call has failed.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see ***context***.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.96.6 Examples

The following example shows how to display the output when a range is specified:

```
[local]Redback#show atm pvc on-demand range 5/1 10:10 through 10:20

Port:Channel      VPI:VCI     through VPI:VCI       Attempts  Success     Failure
5/1 :1            10:10       through  10:20        1         1           0

Authorize Type:                 local
Idle Down Configured:           yes, 30s
Range Created on SARC/PPA:      yes

Failure Statistics:
No shaping profile             0       Shaping profile not found     0
No encap                       0       Non ATM encap                 0
Unsupported ATM encap          0       No binding                    0
No binding applied on range    0       Bad bind type for encap       0
No authen protocols            0       No sub name                   0
No auto-sub name               0       No auto-sub context name      0
Failed auto-sub params         0       PVC exists in RCM             0
Create PVC failure in RCM      0       Delete PVC failure in RCM     0
CCOD range not found in RCM    0       Internal error                0
RCM endpoint down              0       AAA endpoint down             0
RCM restarted                  0       AAA restarted                 0
AAA method failure             0       AAA authorization failure     0
SARC open error                0       SARC close error              0
No memory                      0       TLV failure                   0
System call error              0
```

1.97 show atm summary

show atm summary [**all**]

1.97.1 Purpose

Displays summary information about the Asynchronous Transfer Mode (ATM) ports and permanent virtual circuits (PVCs) that are used for operations, administration, and maintenance (OAM).

1.97.2 Command Mode

All modes

1.97.3 Syntax Description

`all`	Optional. Displays summary information for both bound and unbound PVCs that are used for OAM in any context. This keyword is available only in the local context.

1.97.4 Default

Displays summary information for ATM OAM PVCs that are bound in the current context only.

1.97.5 Usage Guidelines

Use the **`show atm summary`** command to display information about ATM ports and PVCs that are used for OAM.

The **`all`** keyword is available only in the local context and displays summary information for both bound and unbound PVCs that are used for OAM in any context.

If the **`all`** keyword is not specified, only the ATM PVCs that are used for OAM and bound in that context are listed.

Note: By default, most **`show`** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see ***`context`***.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.97.6 Examples

The following example shows how to display the type of information retrieved by the **`show atm summary`** command:

```
[local]Redback#show atm summary
```

```
NO ATM OAM Fault Monitoring Enabled on any PVCs

NO ATM OAM Heartbeat (Continuity) Enabled on any PVCs

NO ATM OAM Auto-loopback Enabled on any PVCs
```

1.98 show atm vp

show atm vp [**profile** *prof-name*] [*slot*/*port* [**vpi** *vpi*]] [**summary**]

1.98.1 Purpose

Displays information about one or more shaped Asynchronous Transfer Mode (ATM) virtual paths (VPs).

1.98.2 Command Mode

All modes

1.98.3 Syntax Description

profile *prof-name*	Optional. Name of an ATM profile.
slot	Optional. Chassis slot number of an ATM traffic card with permanent virtual circuits (PVCs) to be displayed. The range of values depends on the chassis in which the card is installed; see Table 43.
port	Required if you enter the slot argument. Port number with PVCs to be displayed. The range of values depends on the type of traffic card; see Table 44.
vpi *vpi*	Optional. VP identifier (VPI). The range of values is 0 to 255.
summary	Optional. Displays summary information only.

1.98.4 Default

None

1.98.5 Usage Guidelines

Use the **show atm vp** command to display information about one or more shaped ATM VPs.

Table 43 lists the values for the *slot* argument for each type of SmartEdge router; in the table, the IR abbreviation is used for Intermediate Reach.

Table 43 Slot Ranges for ATM Traffic Cards

	slot **Argument Range**	
Traffic Card Type	**SmartEdge 400 Router**	**SmartEdge 800 Router**
8-port ATM OC-3c/STM-1c 2-port ATM OC-12c/STM-4c	1 to 4	1 to 6 and 9 to 14

Note: The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 44 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

Table 44 Port Ranges for ATM Traffic Cards

Traffic Card Type	**Physical Ports**	**Low-Density Version**	**Low-Density Ports**
8-port ATM OC-3c/STM-1c	8	No	–
2-port ATM OC-12c/STM-4c	2	No	–

Note: The value for the *port* argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

If no VPIs are specified, a table of VPs is displayed with a summary line at the end; specify the **summary** keyword to display only the summary line.

Note: If no shaped ATM VPs exist on the port or the system, no output displays.

Note: By default, most **show** commands in any mode display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see *context*.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.98.6 Examples

The following example shows how to display summary information only:

```
[local]Redback#show atm vp summary


Total Shaped VPs: 3 Total VCs in Shaped VPs: 32
```

The following example shows how to display summary information for all shaped ATM VPs on the system:

```
[local]Redback#show atm vp


Port:Channel VPI Total-VCI Profile
 9/1 :1        1         0 atm-ubr
 9/1 :1        5        21 atm-ubr
10/1         211        11 atm-ubr
Total Shaped VPs: 3 Total VCs in Shaped VPs: 32
```