ERICSSON

Commands: am through b

COMMAND DESCRIPTION

Contents

1 Command Descriptions

Commands starting with “am” through commands starting with “b” 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 application

`application` ***`application-name`***

`no application` ***`application-name`***

1.1.1 Purpose

Create an application list of one or more protocol and port definitions and access IP application configuration mode.

1.1.2 Command Mode

Flow IP application list configuration

1.1.3 Syntax Description

`application-name` Specifies a name for the application.

1.1.4 Default

None.

1.1.5 Usage Guidelines

Use the **application** command to create an application list of one or more protocol and port definitions and access IP application configuration mode.

The protocol and port definitions define the application. For example, the TCP-Telnet application could be defined by protocol 6 port 23. In this case, any data that arrives on protocol 6, on port 23 is part of the application TCP-Telnet. You can define up to 63 applications to be tracked in any one application-list.

We recommend defining an application name that corresponds to the protocol statistics you want to display. For example, if you are displaying statistics for the TCP telnet protocol (which has protocol ID 6), you can configure the application name to be TCP-Telnet.

The application name you specify contains one or more IP protocol identifiers and port information you provide with the **protocol** command after you access flow IP configuration mode. You can create multiple flow IP application lists and application names for statistical data collection on IP protocols.

When you enter the **show flow ip cache statistics application** command, the command output displays only statistics that are applicable to the protocols you defined in the application lists.

You cannot configure the same protocol and port number in two separate applications. For example, if protocol 6 is configured under an application called **app-tcp**, you cannot add protocol 6 to the application called **app-udp**, as shown in the following example:

```
[local]Redback(config-flow-ip-app-list)#application app-tcp
[local]Redback(config-flow-ip-app)#protocol 6 port 5200 5400
[local]Redback(config-flow-ip-app-list)# application app-udp
[local]Redback(config-flow-ip-app)#protocol 6 port 5225
```

Use the **no** version of this command to remove an application from an IP application list.

1.1.6 Examples

The following example shows the **application** command used to access flow IP application configuration mode:

```
[local]Redback(config)# flow ip application-list
[local]Redback(config-flow-ip-app-list)# application app1
[local]Redback(config-flow-ip-app)#
```

1.2 application-list

application-list ***application-list-name***

no application-list ***application-list-name***

1.2.1 Purpose

Enables application summary statistics monitoring for an RFlow profile.

1.2.2 Command Mode

Flow IP profile configuration

1.2.3 Syntax Description

application-list-name	Specifies a name for the application list.

1.2.4 Default

System default application list (sys_dflt_app_list_)

1.2.5 Usage Guidelines

Use the **application-list** command to enable application summary statistics monitoring for an RFlow profile.

Use the **no** version of this command to disable application summary statistics monitoring for an RFlow profile.

1.2.6 Examples

The following example shows how to use the **application-list** command to configure the profile **p1** to use the application list TCP-list1. For the flows associated with profile **p1**, the **show flow ip cache statistics application** command output displays only those statistics that are applicable to the applications defined in **TCP-list1_**:

```
[local]Redback#configure
[local]Redback(config)#flow ip profile p1
[local]Redback(config-flow-ip-profile)#applica
tion-list TCP-list1
```

1.3 aps

aps {**protect** | **working**} ***aps/msp-group-name***

no aps {**protect** | **working**}

1.3.1 Purpose

Assigns the port as a working or protect port to an existing Automatic Protection Switching (APS) Multiplex Section Protection (MSP) group.

1.3.2 Command Mode

- ATM OC configuration
- STM-1 configuration
- STM-4 configuration

1.3.3 Syntax Description

protect	Indicates that the port is a protect port in the specified APS MSP group.
working	Indicates that the port is a working port in the specified APS MSP group.
aps/msp-group-name	Unique alphanumeric string used to identify a specific pair of optical ports.

1.3.4 Default

None

1.3.5 Usage Guidelines

Use the **aps** command to assign a port, as a working or protect port, to an existing APS/MSP group. You can add the working and protect ports in any order.

After you add any OC port to an APS/MSP group as a protect port, **description**, **path-trace**, and **shutdown** commands are available for the port.

The following settings are also available under the protect port:

- POS port: c2byte
- Channelized OC port: c2byte
- Channelized STM port: c2byte and au3/au4 submenu

When creating an TDM channel on the Channelized OC or Channelized STM APS working port, the same channel is created automatically on the protect port, and the settings are replicated from the working channel.

Note: The **aps** command applies to Cisco High-Level Data Link Control (HDLC)-encapsulated Packet over SONET/SDH (OC48, OC12, and OC3 POS ports only), Asynchronous Transfer Mode (ATM) OC ports, and channelized SONET/SDH ports (OC ports and STM ports).

Use the **no** form of this command to remove the port from the APS/MSP group and return the port to non-APS/MSP operation.

Caution!

Risk of service disruption. When an APS/MSP working or protect port is deleted from an APS/MSP group, all sessions currently active on the ports are terminated. Only sessions on the working port can be brought back up as normal. To reduce the risk of service disruption beyond this temporary termination of sessions when deleting a working or protect port from an APS/MSP group, perform the procedure provided in *Delete (Unconfigure) a POS Port from an APS/MSP Group*.

Consider the following limitations for APS/MSP groups:

- Removing an ATM port from an APS/MSP group also removes all ATM virtual paths (VPs) and permanent virtual circuits (PVCs) from both the working and protect ports.
- Removing a Channelized OC or Channelized STM port from an APS/MSP group also removes all its TDM channels.
- Ports are rejected from an APS/MSP group when ATM VP or PVC configurations exist or when the TDM channels create a Channelized OC port or Channelized STM port.
- TDM Channels and ATM VP/PVCs only allow configuration on the working port after it is bound to an ASP/MSP group.
- After a working port is removed from an APS group, all settings on that port revert to default values.
- Ports are rejected from an APS/MSP group when any replicated port setting configuration exists.

1.3.6 Example

1.3.6.1 POS Port Example

The following example shows how to configure two ports for the APS/MSP group `lab48:`

```
!Create the APS/MSP group
[local]Redback(config)#aps group lab48 pos
[local]Redback(config-aps)#exit
!Configure the working port
[local]Redback(config)#port pos 1/8
[local]Redback(config-port)#bind interface if-lab48 local
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#exit
!Configure the protect port
[local]Redback(config)#port pos 1/7
[local]Redback(config-port)#aps protect lab48
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#exit
```

1.3.6.2 Channelized Port Example

```
Current configuration:
!
card ch-oc3oc12-8or2-port 11
!
port channelized-stm4 11/1 pos
 ! au3-vc3-tug2-tu12-vc12-c12 mapping
 aug-mapping au3-tu12
 au3 1
 shutdown
 aps working pos9
 !
 port e1 11/1:1
 ! AUG-4 1, AUG-1 1, AU-3 1, TUG-2 1, C12 1
  no shutdown
  bind interface intf6 local
 !
 port e1 11/1:63
 ! AUG-4 1, AUG-1 1, AU-3 3, TUG-2 7, C12 3
  no shutdown
  encapsulation ppp
  bind interface intf7 local
!
port channelized-stm4 11/5 pos
 ! au3-vc3-tug2-tu12-vc12-c12 mapping
 aug-mapping au3-tu12
 no shutdown
 aps protect pos9
 !
 ! ---- aps protect channel
 ! port e1 11/5:1
 ! no shutdown
 !
 ! ---- aps protect channel
 ! port e1 11/5:63
 ! no shutdown
!
```

1.4 aps group

aps group ***aps/msp-group-name*** [**atm** | **pos**]

no aps group ***aps/msp-group-name***

1.4.1 Purpose

Creates an empty Automatic Protection Switching (APS) or MSP (Multiplex Section Protection) group or selects an existing APS/MSP group for modification and accesses APS configuration mode.

1.4.2 Command Mode

Global configuration

1.4.3 Syntax Description

aps/msp-group-name	Unique alphanumeric string used to identify a specific pair of optical ports.
atm	Optional. Creates the APS/MSP group for Asynchronous Transfer Mode (ATM) ports.
pos	Optional. Creates the APS/MSP group for Packet over SONET/SDH (POS) ports. This is the default.

1.4.4 Default

No APS/MSP groups are created.

1.4.5 Usage Guidelines

Use the **aps group** command to create an empty APS/MSP group or select an existing APS/MSP group for modification and access APS configuration mode.

Use the **no** form of this command to delete the specified APS group.

Note: You cannot delete an APS/MSP group if it contains working and protect ports. You must first delete the ports from the group. (For the procedures to delete ports, see *Delete (Unconfigure) a POS Port from an APS/MSP Group*.)

1.4.6 Examples

The following example shows how to create the APS/MSP group `lab48` for POS ports:

```
[local]Redback(config)#aps group lab48 pos
[local]Redback(config-aps)#
```

The following example shows how to create the APS/MSP group `lab49` for ATM ports:

```
[local]Redback(config)#aps group lab49 atm
[local]Redback(config-aps)#
```

1.5 aps switch

aps switch {**force** | **lockout** | **manual**}

no aps switch {**force** | **lockout** | **manual**}

1.5.1 Purpose

Changes the traffic state of a port in an Automatic Protection Switching (APS) or Multiplex Section Protection (MSP) group.

1.5.2 Command Mode

Port configuration

1.5.3 Syntax Description

force	Switches the sessions on the working port to the protect port or the protect port to the working port, unless a request of equal or higher priority is already in effect. This request has high priority.
lockout	Prevents the sessions on the working port from being switched to the protect port.
manual	Switches the sessions from the working port to the protect port or from the protect port to the working port, unless a request of equal or higher priority is already in effect. This request has low priority.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **aps switch** command to change the traffic state of a port in an APS/MSP group. The **aps switch** command persists after the system is reset if the configuration has been saved using the **save configuration** command (in exec mode).

Specify the **force** keyword to switch the sessions on the working port to the protect port or conversely. The request succeeds if no request with higher priority is in effect and remains in effect until it is explicitly cleared with the **no** form of this command or implicitly cleared by a higher-priority request.

Specify the **lockout** keyword to prevent sessions on the working port from being switched to the protect port. A lockout request persists after the system is

reset and remains in effect until it is explicitly cleared with the **no** form of this command or implicitly cleared by a higher-priority request. This keyword is available only for the protect port; it is ignored if you specify it for a working port.

Caution!

Risk of disabling APS/MSP protection. Because the **aps switch force** command has higher priority than signal degrade or signal fail conditions, it can cause sessions to be switched to a nonfunctioning port for the APS/MSP group. To reduce the risk, use caution when using this command, or post a lower-priority request with the **manual** keyword.

Specify the **manual** keyword to switch the sessions on the working port to the protect port or the protect port to the working port. The request succeeds if no request with higher priority is in effect and remains in effect until it is explicitly cleared with the **no** form of this command or implicitly cleared by a higher-priority request.

Note: Ports are rejected from an APS/MSP group when Asynchronous Transfer Mode (ATM) virtual path (VP) or permanent virtual circuit (PVC) configurations exist.

APS/MSP requests (generated either by the system or an administrator) have priority levels, which determine the order in which they are carried out. Lockout is the highest priority APS/MSP request that you can post on a port. If a lockout is in effect and a lower-priority request is posted, it is rejected; however, it is posted, and you must enter the **no** form of this command to clear it. Table 1 describes the relative priority levels, from highest to lowest, for APS/MSP requests.

Table 1 Priority Levels for APS/MSP Requests

Priority	Request	Description	System or Administrator Request
Highest	Lockout	Prevents the working port from being switched to the protect port, unless a request of equal or higher priority (another lockout request) is already in effect.	Administrator

Table 1 Priority Levels for APS/MSP Requests

Priority	Request	Description	System or Administrator Request
	Signal failure on protect port	Is generated by the system if one of the following fatal port error conditions is detected: • Loss of signal • Loss of frame • Line alarm indication signal (AIS-L) is received • Bit error rate (BER) that is received exceeds the configured signal fail (SF-BER) threshold • Port is disabled (port is shut down) • Line card has failed or is removed	Automatic
	Forced	Switches the sessions on the working port to the protect port or on the protect port to the working port, unless a request of equal or higher priority is already in effect.	Administrator
	Signal failure on working port	Is generated by the system if one of the following fatal port error conditions is detected: • Loss of signal • Loss of frame • AIS-L is received • BER that is received exceeds the configured SF-BER threshold • Port is disabled (port is shut down) • Line card has failed or is removed	Automatic
	Signal degrade	BER that is received exceeds the configured signal degradation BER (SD-BER) threshold.	Automatic

Table 1 Priority Levels for APS/MSP Requests

Priority	Request	Description	System or Administrator Request
	Manual	Switches the sessions on the working port to the protect port or on the protect port to the working port, unless a request of equal or higher priority is already in effect.	Administrator
Lowest	Wait to restore	If revertive switching is configured, this switch is generated when a signal failure or signal degrade condition has been cleared and the subsequent wait-to-restore (WTR) timer has expired.	Automatic

Note: If equal priority requests exist on the working and protect ports (for example, if both ports have failed), the APS group switches to the working port.

Use the **no** form of this command to clear the request.

1.5.6 Examples

The following example shows how to lock out protect port `2/1` (disable APS switching), and then remove the lockout:

```
[local]Redback(config)#port pos 2/1
[local]Redback(config-port)#aps protect lab48
[local]Redback(config-port)#aps switch lockout
[local]Redback(config-port)#no aps switch lockout
```

1.6 architecture 1+1

architecture 1+1 [**bidirectional** | **unidirectional**]

{**no** | **default**} **architecture 1+1**

1.6.1 Purpose

Specifies the mode for a linear 1+1 Automatic Protection Switching (APS) or Multiplex Section Protection (MSP) group.

1.6.2 Command Mode

APS configuration

1.6.3 Syntax Description

bidirectional	Optional. Specifies bidirectional mode. This is the default for Packet over SONET/SDH (POS) ATM groups.
unidirectional	Optional. Specifies unidirectional mode. This is the default for Asynchronous Transfer Mode (ATM) APS/MSP groups.

1.6.4 Default

The default mode for an ATM APS/MSP group is unidirectional; the default mode for POS APS/MSP groups is bidirectional.

1.6.5 Usage Guidelines

Use the **architecture 1+1** command to specify the mode for a linear 1+1 APS/MSP group.

The **unidirectional** keyword is supported for ATM APS/MSP groups only and is the default for those groups. The **bidirectional** keyword is supported for both POS and ATM APS/MSP groups and is the default for POS APS/MSP groups.

1.6.6 Examples

The following example shows how to configure a port for the APS/MSP group `lab48:`

```
[local]Redback(config)#aps group lab48 atm
[local]Redback(config-aps)#architecture 1+1 bidirectional
```

1.7 area

area {***area-id*** | ***ip-addr***}

no area {***area-id*** | ***ip-addr***}

1.7.1 Purpose

In OSPF router configuration mode, configures an Open Shortest Path First (OSPF) area and enters OSPF area configuration mode.

In OSPF3 router configuration mode, configures an OSPF Version 3 (OSPFv3) area and enters OSPF3 area configuration mode.

1.7.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.7.3 Syntax Description

area-id	32-bit number. The range of values is 0 to 4,294,967,295. The 0 value is reserved for the backbone area.
ip-addr	IP address. The 0.0.0.0 value is reserved for the backbone area.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **area** command (in OSPF router configuration mode) to configure an OSPF area and enter OSPF area configuration mode.

Use the **area** command (in OSPF3 router configuration mode) to configure an OSPFv3 area and enter OSPF3 area configuration mode.

Multiple areas are supported per OSPF or OSPFv3 instance. Specify the area ID or IP address for the router to use when participating in OSPF or OSPFv3 routing. All routers in an area must use the same area ID to establish neighbor adjacencies.

To specify that the router is directly connected to the OSPF or OSPFv3 backbone, use the **area 0.0.0.0** or **area 0** construct.

Use the **no** form of this command to remove an OSPF or OSPFv3 area.

1.7.6 Examples

The following example shows how to configure an area using an IP address of `34.0.0.0` and enter OSPF router configuration mode:

```
[local]Redback(config-ospf)#area 34.0.0.0
[local]Redback(config-ospf-area)#
```

1.8 area-type

area-type {**nssa** [**no-redistribution**] [**no-default**] | **stub** [**no-summary**]}

{**no** | **default**} **area-type**

1.8.1 Purpose

Defines an Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) area as a stub area or not-so-stubby-area (NSSA).

1.8.2 Command Mode

- OSPF area configuration
- OSPF3 area configuration

1.8.3 Syntax Description

nssa	Configures the area as an NSSA.
no-redistribution	Optional. Suppresses redistribution of non-OSPF routes by an autonomous system border router (ASBR) into an NSSA area. By default, redistributed routes are advertised using Type 7 link-state advertisements (LSAs).
no-default	Optional. Suppresses NSSA default origination. An NSSA area border router (ABR) normally advertises a type 7 or type 3 default LSA in the NSSA. This keyword suppress the default.
stub	Configures the area as a stub type.
no-summary	Optional. Suppresses the advertisement of Type 3 LSAs, or interarea routes, into a stub area. This option is only relevant when the router is configured as an ABR.

1.8.4 Default

The area type is normal.

1.8.5 Usage Guidelines

Use the **area-type** command to define an OSPF or OSPFv3 area as a stub area or as an NSSA.

A stub area relies on default routing to forward traffic addressed to external destinations. You cannot configure the backbone as a stub area.

Use the **no** or **default** form of this command to return the specified area to a normal area.

1.8.6 Examples

The following example shows how to configure `area 4` as a stub area:

```
[local]Redback(config-ospf)#area 4
[local]Redback(config-ospf-area)#area-type stub
```

1.9 arp rate

arp rate *pps* **burst** *packets*

1.9.1 Purpose

Creates a rate limit and burst threshold for incoming Address Resolution Protocol (ARP) packets.

1.9.2 Command Mode

Protocol-rate-limit policy configuration

1.9.3 Syntax Description

pps	Rate in packets per second. The range of values is 1 to 2,500,000.
burst *packets*	Burst tolerance in packets. The range of values is 1 to 25,000,000.

1.9.4 Default

No rate limit or burst threshold is configured for incoming ARP packets.

1.9.5 Usage Guidelines

Use the **arp rate** command to create a rate limit and burst threshold for incoming ARP packets.

You set the ARP rate limit and burst threshold when configuring a protocol-specific rate-limiting policy, which you can then apply to a subscriber record, PVC, port, or link group. Use the **qos policy protocol-rate-limit** command in global configuration mode to configure the policy. Then, use the command in subscriber, ATM PVC, 802.1Q PVC, port, or link-group configuration mode to bind it to an entity.

1.9.6 Examples

The following example shows how to create and configure the **ARPDOS** policy and apply it to Ethernet port 5/1:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#port ether 5/1
[local]Redback(config-port)#qos policy protocol-rate-limit ARPDOS
```

The following example creates and configures the ARPDOS policy and applies it to subscriber circuits where the default subscriber profile is applied:

```
[local]Redback(config)#qos policy ARPDOS protocol-rate-limit
[local]Redback(config-policy-protocol)#arp rate 5000 burst 100000
[local]Redback(config-policy-protocol)#exit
[local]Redback(config)#subscriber default
[local]Redback(config-sub)#qos policy protocol-rate-limit ARPDOS
```

1.10 ascend-data-filter

ascend-data-filter

ipv6-in-forward

no ascend-data-filter

1.10.1 Purpose

Specifies that the ascend-data-filter is applied to IPv6 packets.

1.10.2 Command Mode

Subscriber configuration.

1.10.3 Syntax Description

ipv6-in-forward	Specifies the filter action of the inbound IPv6 traffic to the SmartEdge router.

1.10.4 Default

None.

1.10.5 Usage Guidelines

A RADIUS Access-Accept packet contains multiple binary strings, each representing a rule in an IP access control list (ACL). Use the **ascend-data-filter** command to interpret rules received from the RADIUS server.

1.11 asloop-in

asloop-in ***loop-count***

no asloop-in

1.11.1 Purpose

Disables the AS_PATH loop detection by accepting a route advertisement that contains the local autonomous system number (ASN) in the AS_PATH attribute.

1.11.2 Command Mode

BGP neighbor configuration

1.11.3 Syntax Description

loop-count	Number of times that the local ASN can appear in the AS_PATH attribute. Valid values are 1 to 10.

1.11.4 Default

The AS_PATH loop detection is enabled.

1.11.5 Usage Guidelines

Use the **asloop-in** command to disable the AS_PATH loop detection by accepting a route advertisement that contains the local ASN in the AS_PATH attribute.

Because enabling the **asloop-in** command disables AS_PATH loop detection, it must only be used for specific applications that require this type of behavior, and in situations with strict network control. One application for this command is the Border Gateway Protocol/Multiprotocol Label Switching Virtual Private Network (BGP/MPLS VPN) hub-and-spoke configuration, in which a hub provider edge (PE) router may receive routes containing its own ASN from a hub customer edge (CE) router. To disable AS_PATH loop detection, use the **asloop-in** command on the exporting context of the hub PE router.

The **asloop-in** command is useful only when Border Gateway Protocol is used for PE-to-CE routing.

Note: For a CE router to send a route advertisement back to the PE router from which the route is learned, the CE router must be configured as a BGP peer with the PE router configured as a member of the peer group. By default, routes are not sent back to the neighbor autonomous system (AS) from where they are received.

Use the **no** form of this command to enable the AS_PATH loop detection.

1.11.6 Examples

The following example shows how to enable BGP on a PE router to accept routes with the ASN `100` in the AS_PATH attribute up to `2` times from peer `2.2.2.1:`

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#exit
[local]Redback(config-ctx)#context bar vpn-rd 20.21.22.23:200
[local]Redback(config-ctx)#router bgp vpn
[local]Redback(config-bgp)#address-family ipv4 unicast
[local]Redback(config-bgp-af)#export route-target 300:400
[local]Redback(config-bgp-af)#exit
[local]Redback(config-bgp)#neighbor 2.2.2.1 external
[local]Redback(config-bgp-neighbor)#remote-as 64001
[local]Redback(config-bgp-neighbor)#asloop-in 2
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
```

1.12 as-override

as-override

no as-override

1.12.1 Purpose

Replaces all occurrences of a peer's autonomous system number (ASN) in the AS_PATH attribute of a route with the local ASN, when advertising the route to the peer.

1.12.2 Command Mode

BGP neighbor configuration.

1.12.3 Syntax Description

This command has no keywords or arguments.

1.12.4 Default

The peer's ASN is not replaced by the local ASN.

1.12.5 Usage Guidelines

Use the **as-override** command to replace all occurrences of a peer's ASN in the AS_PATH attribute of a route with the local ASN, when advertising the route to the peer.

When multiple Virtual Private Network (VPN) sites share the same ASN, enabling the AS override feature allows routes originating from an autonomous system (AS) to be accepted by a router residing in the same AS. By default, the receiving router rejects the received route advertisement if the AS_PATH attribute shows that the route originated from its own AS to prevent routing loops.

The **as-override** command can only be used in VPN contexts.

The **as-override** command is useful only when Border Gateway Protocol (BGP) is used for provider edge-to-customer edge (PE-to-CE) routing.

Enabling the AS override feature may result in route loops. This feature should only be used for specific applications that require this type of behavior, and in situations with strict network control.

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

1.12.6 Examples

The following example shows how to replace all occurrences of ASN `64001` in the AS_PATH attribute with the local router's ASN `100` when advertising the routes to peer `1.1.1.1`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-ctx)#exit
[local]Redback(config)#context vpn123 vpn-rd 10.11.12.13:100
[local]Redback(config-ctx)#router bgp vpn
[local]Redback(config-bgp)#neighbor 1.1.1.1 external
[local]Redback(config-bgp-neighbor)#remote-as 64001
[local]Redback(config-bgp-neighbor)#as-override
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
```

1.13 as-path-list (BGP)

as-path-list ***apl-name*** {**in** | **out**}

no as-path-list ***apl-name*** {**in** | **out**}

1.13.1 Purpose

Filters Border Gateway Protocol (BGP) routing updates from or to the specified BGP neighbor or peer group address family.

1.13.2 Command Mode

- BGP neighbor address family configuration
- BGP peer group address family configuration

1.13.3 Syntax Description

apl-name	Autonomous system (AS) path list name.
in	Applies the filter to incoming routes from the BGP neighbor.
out	Applies the filter to outgoing routes to the BGP neighbor. This keyword only applies in BGP neighbor address family configuration mode.

1.13.4 Default

None

1.13.5 Usage Guidelines

Use the **as-path-list** command to filter the BGP routing updates from or to the specified BGP neighbor or peer group address family. Use the **in** keyword to filter the BGP incoming routes from the specified BGP neighbor or peer group. Use the **out** keyword to filter outgoing routes to the BGP neighbor or peer group. The content of the filter list is based on the AS path, which is defined through the **as-path-list** command in context configuration mode.

Note: The **out** keyword 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.

Caution!

Risk of unfiltered routes. If a filter list is applied to a BGP neighbor, but there is no corresponding as path list in context configuration mode, routes are not filtered. To reduce the risk, verify that an AS path list has been configured before applying it to a BGP neighbor.

Currently, AS path list changes automatically take effect, and issuing the **clear bgp neighbor** *ip-addr* **soft** [**in** | **out**] command in exec mode to update an AS path list can cause updates to be unnecessarily sent; therefore, it is not recommended.

To aggregate multiple policy changes, such as the AS path list, the SmartEdge router performs the automatic update 15 seconds after any routing policy has changed.

Note: If the remote peer does not support the BGP route refresh capability, an inbound policy change for the peer will result in an automatic hard reset of the session.

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

1.13.6 Examples

The following example shows how to permit only unicast routes that originate in `AS 101` coming from the BGP neighbor at IP address `102.210.210.1`. In addition, the SmartEdge router sends all multicast BGP routes, except for those routes that belong to AS `202`, to the neighbor at IP address `68.68.68.68:`

```
[local]Redback(config-ctx)#as-path-list filter-101
[local]Redback(config-as-path-list)#permit _101$
[local]Redback(config-as-path-list)#exit
[local]Redback(config-ctx)#as-path-list filter-202
[local]Redback(config-as-path-list)#deny _202_
[local]Redback(config-as-path-list)#permit .*
.
.
.
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#remote-as 200
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#as-path-list filter-101 in
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 68.68.68.68 external
[local]Redback(config-bgp-neighbor)#remote-as 300
[local]Redback(config-bgp-neighbor)#address-family ipv4 multicast
[local]Redback(config-bgp-peer-af)#as-path-list filter-202 out
```

1.14 as-path-list (context configuration)

as-path-list *apl-name*

no as-path-list *apl-name*

1.14.1 Purpose

Creates a Border Gateway Protocol (BGP) autonomous system (AS) path list and enters AS path list configuration mode.

1.14.2 Command Mode

Context configuration

1.14.3 Syntax Description

apl-name	Name of the AS path list.

1.14.4 Default

There are no preconfigured AS path lists.

1.14.5 Usage Guidelines

Use the **as-path-list** command to create a BGP AS path list and enter AS path list configuration mode where you can define conditions using the **permit** and **deny** commands.

You can specify an AS path list filter on both inbound and outbound BGP routes. Each filter is based on regular expressions. If the regular expression matches the representation of the AS path of the route as a set of AS numbers (ASNs), the **permit** or **deny** keyword applies. The AS path does not contain the local ASN. Apply the AS path list to a route map using the **match as-path-list** command. Apply the route map as appropriate.

A regular expression is a pattern that is matched against an input string. A regular expression contains the criteria shown in Table 2.

Table 2 Filter Expression Criteria

Criteria	Description
range	A sequence of characters contained within left and right square brackets; for example, [abcd].

Table 2 Filter Expression Criteria

Criteria	Description
atoms	One of the following single characters: **.** matches any single character. **$** matches the end of the input string. **^** matches the beginning of the input string. ***character*** matches the character. **-** matches a comma (,), left brace ({), right brace (}), the beginning of the input string, the end of the input string, or a space.
piece	One of the following symbols: ***** matches 0 or more sequence of the atom. **+** matches 1 or more sequences of the atom. **?** matches the atom or the null string.
branch	Zero or more concatenated pieces.

The following examples display regular expressions:

```
_100_(via AS100)
^100$(origin AS100)
^100.* (coming from AS100)
```

Use the **no** form of this command to remove an AS path list.

1.14.6 Examples

The following examples shows how to create an AS path list, `aspath-1`, and enter AS path list configuration mode:

```
[local]Redback(config-ctx)#as-path-list aspath-1
[local]Redback(config-as-path-list)#
```

1.15 atm mode

atm mode {**atm-priority** | **ip-priority** | **vc-fair** | **hsvc-fair**}

{**no** | **default**} **atm mode** [**atm-priority** | **ip-priority** | **vc-fair** | **hsvc-fair**]

1.15.1 Purpose

Specifies the mode in which the segmentation and reassembly (SAR) image in the second generation ATM OC line card, or MIC performs traffic shaping and scheduling for virtual paths (VPs) and the permanent virtual circuits (PVCs) configured on them.

1.15.2 Command Mode

- Card configuration
- MIC configuration

1.15.3 Syntax Description

atm-priority	Specifies ATM priority scheduling with shaping, using traffic classes
ip-priority	Specifies IP priority scheduling with shaping, using limited traffic classes.
vc-fair	Specifies weighted round-robin scheduling with shaping, using traffic classes; default mode.
hsvc-fair	Specifies hierarchical shaping with VC fairness; applies to the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM-OC-12c/STM-4c (atm-oc12e-2-port) cards only.

Note: Only the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM-OC-12c/STM-4c (atm-oc12e-2-port) cards support the vc-fair and hsvc-fair ATM modes.

1.15.4 Default

Traffic scheduling is performed using the VC fairness mode.

1.15.5 Usage Guidelines

Use the **atm mode** command to specify the mode in which the SAR image in the second generation ATM OC line card performs traffic shaping and scheduling for VPs and the PVCs configured on them.

Note: A PVC created on a shaped VP is referred to as a virtual circuit (VC) in the following descriptions of the modes, only to easily distinguish it from a PVC configured on a nonshaped VP.

Possible modes are:

- ATM priority

This mode supports different ATM profiles with different shaping for VPs and the ATM VCs that you configure on them. VPs and VCs are shaped using constant bit rate (CBR), variable bit rate-real time (VBR-rt), VBR nonreal-time (VBR-nrt), or unspecified bit rate (UBR), subject to the restrictions in *Configuring ATM*.

This mode uses these traffic classes to perform VP and VC scheduling; VCs can also be scheduled with an attached quality of service (QoS) ATM weighted fair queuing (WFQ) scheduling policy.

PVCs configured on a nonshaped VP are shaped using any traffic class, including UBR extended (UBRe), and can be scheduled using traffic classes and an attached QoS ATMWFQ scheduling policy.

The ATM priority mode is not available on the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM-OC-12c/STM-4c (atm-oc12e-2-port) cards.

- IP priority

  This mode supports different profiles with different shaping for VPs and their VCs, but restricts the shaping for VPs to CBR, UBR with the peak cell rate (PCR) option, VBR-rt, and VBR-nrt; VCs are restricted to UBR with the PCR option.

  The IP priority mode is not available on the 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM-OC-12c/STM-4c (atm-oc12e-2-port) cards.

  This mode uses the IP priorities specified by an attached QoS ATMWFQ policy to perform VP and VC scheduling.

  Note: If the QoS ATMWFQ policy has queue 0 mode set to alternate, the PVC that policy is configured on is treated as low priority. We recommend using strict mode for IP priority to work properly.

  PVCs configured on a nonshaped VP are shaped using any traffic class except UBRe, and can be scheduled using traffic classes and an attached QoS ATMWFQ scheduling policy. (Configuring PVCs in this mode is not recommended.)

  Note: The ATM priority and IP priority modes reduce the number of PVCs that you can configure on a second generation ATM OC line card.

- VC fairness

  This mode supports different profiles with different shaping for shaped VPs and their VCs, but restricts the shaping for VPs to CBR, UBR with the PCR option, VBR-rt, and VBR-nrt; VCs are restricted to UBR without the PCR option.

This mode uses traffic classes to perform VP scheduling; VCs are scheduled using weighted round-robin (WRR) scheduling. VCs can also be scheduled with an attached QoS ATMWFQ scheduling policy.

PVCs configured on a nonshaped VP are shaped and scheduled using any traffic class.

- HSVC fairness

  This mode supports the same functionality as VC fairness, is not restricted to UBR without the PCR option; and supports up to 8 queues, port rate limiting, and VC fairness under congestion.

For more information about shaping, traffic classes, and traffic scheduling, see *Configuring ATM*. For more information about IP priorities, class of service (CoS) queues, and QoS ATMWFQ policies, see *Configuring Queuing and Scheduling*.

Note: The ATM priority mode replaces the hierarchical-shaped virtual circuit (HSVC) SAR image that was supported in previous releases. Second-generation ATM OC line cards that were configured with the **`hierarchical shaping`** command (in card configuration mode) are automatically configured by using this command with the **`atm-priority`** keyword.

You cannot enter this command for a second-generation ATM OC line card for which you have already configured ATM VPs or ATM PVCs. You must remove the VPs and PVCs with one of the following commands before you can specify a different mode:

- The **`no`** form of the **`atm vp`** and **`atm pvc`** commands (in ATM OC configuration mode)
- The **`no`** form of the **`port atm`** command (in global configuration mode) for each port that has VPs and PVCs configured
- The **`no`** form of the **`card`** command (in global configuration mode) or the no form of the **`mic`** command (in card configuration mode).

If you attempt to specify an ATM mode that is different from the current mode, the system displays a warning message; you must commit the transaction using the **`commit`** command (in any configuration mode) to change the mode. You can the delete the transaction by entering the **`abort`** command (in any configuration mode) to terminate the operation without changing the mode.

Caution!

Risk of data loss. This command causes a card reload, which disrupts all traffic on the card. To reduce the risk, do not change the mode of the card during peak traffic times.

To view the current mode in a second-generation ATM OC line card or a MIC, enter the **show hardware** command (in any mode) with the **card** and **detail** keywords; the mode displays in the SAR Image Type field. For information about this command, see *Managing Hardware*.

Use the **no** or **default** form of this command to specify the default mode. The same restrictions apply to the **no** and **default** forms of this command as the command itself:

- You must remove all ATM VPs and ATM PVCs configured for the card or MIC before changing the mode as described previously.
- You must enter the **commit** command (in card configuration mode) for the change of mode to proceed.

1.15.6 Examples

The following example shows how to specify the ATM priority mode for a 8-port ATM OC-3c/STM-1c line card for which no ATM VPs or PVCs are configured:

```
[local]Redback(config)#card atm-oc3e-8-port 5
[local]Redback(config-card)#atm mode atm-priority

Note: enable atm-priority SAR image will cause card reload
commit to continue; abort to exit without change

[local]Redback(config-card)#commit
```

The following abbreviated example shows how to display the current mode and its version in the 8-port ATM OC-3c/STM-1c line card in slot 5:

```
[local]Redback(config)#show hardware card 5 detail
```

```
Slot              : 5              Type             : atm-oc3e-8-port

.
.
.
.
Ports Entitled    : All

SAR Image Type    : atm-priority

SAR Image Version : 1.3.33.10.15

Active Alarms     : NONE

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

The following example shows how to specify ATM priority mode for a 8-port ATM OC-3c/STM-1c line card for which one or more ATM VPs or PVCs are configured:

```
[local]Redback(config)#card atm-oc3e-8-port 5
[local]Redback(config-card)#atm mode atm-priority

Cannot modify atm-priority SAR Image Type on card atm-oc3e-8-port in slot 5
: VPs or PVCs exist - remove all VPs and PVCs from this card first
[local]Redback(config-card)#exit
[local]Redback(config)#no port atm 5/1
```

The following example shows how to specify SAR Image Type for a 8-port ATM OC-3c/STM-1c line card in slot 2:

```
[local]Redback(config)#card atm-oc3-8-port 2
[local]Redback(config-card)#atm mode hsvc-fair
[local]Redback(config-card)#commit
[local]Redback(config-card)#exit
```

The following example shows how to specify the default mode for a 8-port ATM OC-3c/STM-1c line card for which no ATM VPs or PVCs are configured:

```
[local]Redback(config)#card atm-oc3e-8-port 5
[local]Redback(config-card)#no atm mode

Note: disable atm-priority SAR image will cause card reload
commit to continue; abort to exit without change

[local]Redback(config-card)#commit
```

1.16 atm profile

atm profile *prof-name* [**static**]

no atm profile *prof-name*

1.16.1 Purpose

Creates a new Asynchronous Transfer Mode (ATM) profile, or selects an existing one for modification, and enters ATM profile configuration mode.

1.16.2 Command Mode

Global configuration

1.16.3 Syntax Description

prof-name	Alphanumeric string used as the name of the particular profile.
static	Optional. Specifies that a profile is to be created or modified to a static profile.

1.16.4 Default

No ATM profiles are defined.

1.16.5 Usage Guidelines

Use the **atm profile** command to create a new ATM profile, or select an existing one, and enter ATM profile configuration mode.

Use the **static** keyword to create a static ATM profile, or to modify an existing dynamic (nonstatic) ATM profile to convert it to a static profile.

You can convert an existing dynamic profile to a static one even if there are ATM VPs and PVCs that reference that profile; the conversion does not affect the VPs and PVCs that reference it. However, you cannot convert a static profile to a dynamic one; instead, you must delete it. Deleting a profile also deletes all VPs and PVCs that reference it.

Note: You must create an ATM profile before you can configure ATM PVCs or VPs that reference that profile.

Note: To assign a static or dynamic (nonstatic) profile dynamically to an ATM PVC, either by using subscriber-specific RADIUS attributes at the time a subscriber session becomes active, or by using the RADIUS Refresh function, you must have enabled the software license for dynamic services. For more information about enabling software licenses, see *Performing Basic System Tasks*.

Do not change traffic class for an ATM profile that is referenced by an ATM VP without first deleting all ATM PVCs configured on that ATM VP. If an error message is displayed when you attempt to change the traffic class of the profile, you must then:

- Use the **no** form of the **atm pvc** command (any of its forms) (in ATM OC configuration mode) to delete the ATM PVCs on all ATM VPs that reference that profile.
- Use the **shaping** command (in ATM profile configuration mode) to specify the new traffic class and its parameters.
- Use the **atm pvc** command (any of its forms) (in ATM OC configuration mode) to recreate the ATM PVCs on all ATM VPs that reference that profile.

  Note: For more configuration guidelines for ATM profiles, VPs, and PVCs, see *ATM Configuration Guidelines* in *Configuring Circuits*.

Use the **no** form of this command to delete an ATM profile.

Caution!

Risk of data loss. This form deletes any ATM VPs and the PVCs on those VPs or any PVCs that reference that profile.

1.16.6 Examples

The following example shows how to create an ATM profile, `low_rate`, and enters ATM profile configuration mode:

```
[local]Redback(config)#atm profile low_rate
[local]Redback(config-atm-profile)#
```

The following example shows how to modify the ATM profile, `low_rate`, to make it a static profile and enter ATM profile configuration mode:

```
[local]Redback(config)#atm profile low_rate static

[local]Redback(config-atm-profile)#end
```

1.17 atm pvc

For a single static Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), the syntax is:

atm pvc *vpi vci* [**profile** *prof-name* **encapsulation** *encaps-type*]

no atm pvc *vpi vci* [**profile** *prof-name* **encapsulation** *encaps-type*]

For a range of static ATM PVCs, the syntax is:

atm pvc explicit *start-vpi*:*start-vci* **through** *end-vpi*:*end-vci*[**profile** *prof-name* **encapsulation** *encaps-type*]

no atm pvc explicit *start-vpi*:*start-vci* **through** *end-vpi*:*end-vci* [**profile** *prof-name* **encapsulation** *encaps-type*]

For a range of ATM PVCs to be created on demand, the syntax is:

atm pvc on-demand *start-vpi*:*start-vci* **through** *end-vpi*:*end-vci* {[**profile** *prof-name* **encapsulation** *encaps-type*] | **aaa context** *ctx-name* [**prefix-string** *text* |**user-name** *subscriber*]}

no atm pvc on-demand *start-vpi*:*start-vci* **through** *end-vpi*:*end-vci* [[**profile** *prof-name* **encapsulation** *encaps-type*] | **aaa context** *ctx-name* [**prefix-string** *text* |**user-name** *subscriber*]]

1.17.1 Purpose

Configures one or more ATM PVCs, or selects one or more PVCs for modification, and enters ATM PVC configuration mode.

1.17.2 Command Mode

- ATM OC configuration

1.17.3 Syntax Description

vpi	Virtual path identifier (VPI) for the virtual path (VP) when creating or modifying a single PVC. The range of values is 0 to 255.
vci	Virtual circuit identifier (VCI) when creating or modifying a single PVC. The range of values is 1 to 65,535. By convention, values 1 to 31 are reserved for system use.
start-vpi	First virtual path identifier (VPI) when creating or modifying a range of PVCs. The range of values is 0 to 255.
start-vci	First virtual circuit identifier (VCI) when creating or modifying a range of PVCs. The range of values is 1 to 65,535. By convention, values 1 to 31 are reserved for system use.
through	Specifies the end of the range.
end-vpi	Last VPI in the range of VPs for the range of PVCs to be configured. The range of values is 0 to 255.
end-vci	Last VCI in a range of PVCs to be configured. The range of values is 1 to 65,535. By convention, values 1 to 31 are reserved for system use.
profile ***prof-name***	Optional. Existing ATM profile. Optional only when selecting an existing PVC or range of PVCs for deletion or modification.
encapsulation ***encaps-type***	Optional. Specific encapsulation type, according to one of the keywords listed in Table 3. Optional only when selecting an existing PVC or range of PVCs for deletion or modification.
on-demand	Specifies a listening PVC or range of PVCs; a listening PVC is created in memory only after traffic is detected on it.
aaa	Optional. Specifies that the profile for the PVCs is assigned dynamically, using authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS). Optional only when selecting an existing PVC or range of PVCs for deletion or modification.
context ***ctx-name***	Name of the context in which are configured the RADIUS servers that are used to provide the encapsulation type and ATM profile for the on-demand ATM PVCs.
prefix-string ***text***	Optional. String to be used as a prefix in constructing the User-Name attribute. Must not contain spaces, periods, underscores, or forward or backward slashes.
user-name ***subscriber***	Optional. String to be used for the subscriber name, in any valid structured subscriber name format; it can be up to 253 characters.

1.17.4 Default

No ATM PVCs are configured.

1.17.5 Usage Guidelines

Use the **atm pvc** command to configure one or more ATM PVCs, or select one or more PVCs for modification, and enter ATM PVC configuration mode. This command has the following forms:

- Use the **atm pvc** form of the command to configure a single explicitly configured (static) ATM PVC, or to select one for modification, and enter ATM PVC configuration mode.
- Use the atm pvc explicit form of the command to configure a range of static PVCs with similar characteristics, or to select the range for modification.
- Use the atm pvc on-demand form of the command to configure a range of on-demand PVCs, with similar characteristics, each of which is made active only when user traffic is detected on it.

Caution!

Risk of data loss. By convention, VCIs 1 to 31 are solely for system use, and any user data is overwritten. To reduce the risk, create VCI 4 only in connection with the **oam fault-monitor** or **oam manage** commands.

Table 3 lists the keywords for the ***encaps-type*** argument.

Table 3 Types of ATM Encapsulations

Keyword	Description
bridge1483	Specifies RFC 1483 bridged encapsulation.
cell	Specifies ATM cell mode encapsulation.
multi	Specifies multiprotocol encapsulation. Use this option to create PVCs on which you create child circuits.
ppp	Specifies VC-multiplexed.
ppp auto	Enables the auto-detect feature with regard to the PPP encaps type.
ppp llc	Specifies Logical Link Control-Subnetwork Access Protocol (LL PPP encapsulation as defined in RFC 2364, `PPP over AAL5`
ppp nlpid	Specifies Network Layer Protocol Identifier (NLPID) PPP encap
ppp serial	Specifies Serial High-Level Data Link Control (HDLC) PPP encapsulation—used in non-RFC-compliant configurations.

Keyword	Description
pppoe	Specifies PPP over Ethernet (PPPoE) encapsulation.
raw	Specifies raw mode. Raw encapsulation mode strips the pa Layer 2 headers and allows switching raw encapsulation mo without Layer 2 processing. See *Configuring Cross-Connec*
route1483	Specifies RFC 1483 routed encapsulation.

(1) QoS configuration options are not available for ATM PVCs in raw encapsulation mode.

The following guidelines apply to encapsulation types:

- You cannot change the encapsulation of a PVC unless you first delete it, and then recreate it.
- RFC 1483 bridged encapsulation (**bridge1483** keyword) requires a local medium access control (MAC) address and the MAC address of the remote host. The operating system provides these MAC addresses as follows:
  - The default local MAC address for the port is extracted from the EEPROM of the line card when the card is installed in the SmartEdge chassis. You can override this address by entering the **mac-address** command (in ATM OC configuration mode).
  - You can associate the MAC address of the remote host with the ATM PVC by entering the **ip host** command (in ATM PVC configuration mode).
- The following restrictions apply to ATM cell mode encapsulation (**cell** keyword):
  - ATM cell mode encapsulation supported only on ATM cards running in the default vc-fair mode.
  - ATM cell mode encapsulation is not supported on the SmartEdge 100 router media interface cards (MICs).
  - ATM cell mode encapsulation is supported on ATM OC cards only.
- The **multi** keyword configures the parent PVC to carry IPoE traffic. The following guidelines apply:
  - This keyword is applicable only to PVCs that have child circuits to carry PPPoE, but IPoE version 6 (IPv6oE) traffic is limited to explicit ATM PVCs. To create child circuits on multiprotocol ATM PVCs, use the **circuit protocol** command (in ATM PVC configuration mode); to cross-connect them, see *Configuring Cross-Connections*.
  - You must configure the interface to which you bind the IPoE traffic with the **multibind** keyword. Binding types include static (**bind interface** or **bind subscriber** command in ATM PVC configuration mode) for ATM PVC (IPoE) parent circuit. For PPPoE

child circuits, binding types supported are static (**bind subscriber**) and dynamic (**bind authentication**).

– PVCs with multiprotocol encapsulation are supported on all ATM line cards, and in port listening mode, if enabled.

- If you specify the **ppp auto** construct, the commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. The operating system handles the information entered in these commands appropriately, after the encapsulation is auto-detected.

The following guidelines apply to the **atm pvc explicit** form of this command:

- The range you specify must not overlap or encompass any range of PVCs created previously with the **atm pvc explicit** form of the command; it can include PVCs previously created with the **atm pvc** form of the command.

- The range of PVCs can be on a range of ATM VPs.

- Any PVCs in the specified range that do not already exist are created with the specified profile and encapsulation.

- The range of PVCs can be on a range of ATM VPs. However, an error message is displayed if the range includes VCIs 3 or 4. These VCIs are reserved for operations, administration, and maintenance (OAM) use. In general, avoid specifying VCIs 1 to 31.

- You cannot use the **no atm pvc** command to remove PVCs from an explicit range, but you can use the **atm pvc** form of the command to overwrite one or more PVCs created by the **atm pvc explicit** form of the command. If you subsequently use the **no atm pvc** command to delete such a PVC, the PVC reverts to the **atm pvc explicit** definition.

- You cannot use the **bind subscriber** and **ip host** commands with the PVCs created by the **atm pvc explicit** form of the command; however, if you first modify individual PVCs in the range with the **atm pvc** form of the command, you can then use the **bind subscriber** and **ip host** commands with the modified PVCs.

- When you use the no form of the **atm pvc explicit** form of the command, all the PVCs in the range are deleted except for those in the range that were explicitly created with the **atm pvc** form of the command.

The following guidelines apply to the **atm pvc on-demand** form of this command; be aware that on-demand PVC configuration does not support more PVCs than static PVC configuration supports, although on-demand configuration does conserve memory:

- Raw mode encapsulation is not supported for on-demand PVCs.

- Otherwise, the range that you specify must be within the limits for active PVCs; these limits depend upon the type of port, the SAR image for the card, and the traffic class specified by the profile. An error message is displayed if the range that you specify is not supported; see the tables that specify PVC limits based on SAR image in *Maximum Number of ATM PVCs and VPs*.

  Note: Enabling port listening mode with the **`ccod-mode port-listen`** command must precede the configuration of any ATM VPs or PVCs on that ATM port.

- The range of PVCs can be on a range of ATM VPs. However, an error message is displayed if the range includes VCIs 3 or 4. These VCIs are reserved for operations, administration, and maintenance (OAM) use. In general, avoid specifying VCIs 1 to 31.

- Regardless of the number of listening PVCs that you create, the number of active PVCs cannot be greater than those specified for each traffic class and SAR image on the type of port on which they are created; see the tables that specify PVC limits based on SAR image in *Maximum Number of ATM PVCs and VPs*.

- You cannot overwrite a PVC range that you previously configured with the **`atm pvc explicit`** or **`atm pvc on-demand`** form of the command, unless the new range completely encompasses that previous range.

- If you overwrite a PVC range that was previously defined with the **`atm pvc explicit`** form of the command, the circuits are not cleared. You must use the clear atm circuit command to manually clear these circuits.

- If you overwrite an on-demand PVC with the **`atm pvc`** form of the command and subsequently delete such a PVC with the **`no atm pvc`** command, the PVC reverts to the **`atm pvc on-demand`** definition.

- You cannot use the **`no atm pvc`** command to remove PVCs from a range of on-demand PVCs.

- When you create a range of on-demand PVCs, you can:

  – Use the profile and encapsulation keywords to specify the profile and encapsulation type explicitly.

  – Use the **`aaa`** keyword to use AAA and RADIUS to assign the profile, encapsulation, and binding of the PVCs in the range at the time the PVC becomes active.

- If you use the **`aaa`** keyword, you must include the **`context`** ***`ctx-name`*** construct to specify the context in which the RADIUS server is configured. You can also define a prefix string that is used to construct the User-Name attribute.

By default, the RADIUS User-Name attribute is in the form ***hostname.port.slot.vpi.vci***. If you define a prefix string, the RADIUS User-Name attribute is in the form ***prefix-string.vpi.vci***.

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

- The ***subscriber*** argument can include both the subscriber name and the domain name in any valid format, such as ***sub-name@ctx-name***, but it must match an entry in the RADIUS user database. The format, including the separator character, is configurable; for information about configuring the format, see *Configuring Authentication, Authorization, and Accounting*.

  Note: If you assign a static or dynamic (nonstatic) profile dynamically to an ATM PVC, either by using subscriber-specific RADIUS attributes at the time a subscriber session becomes active, or by using the RADIUS Refresh function (the **aaa** keyword), you must have enabled the software license for dynamic services. For more information about enabling software licenses, see *Performing Basic System Tasks*.

  Note: For more configuration guidelines for ATM profiles, VPs, and PVCs, see *Configuring ATM, Ethernet, and POS Ports*.

Use the **no** form of this command to delete a previously created PVC or range of PVCs; when deleting a range of PVCs, you must specify the same circuit range as specified in the **atm pvc explicit** or **atm pvc on-demand** form of the command. If you specify the optional constructs, the system checks the PVC configuration against the input arguments and does not delete the PVC or range of PVCs unless there is a match.

1.17.6 Examples

The following example shows how to configure a static PVC that references a previously defined ATM profile, `dslam1`, an encapsulation of `bridge1483`, and a VPI:VCI of `0:32` on an ATM OC port:

```
[local]Redback(config)#port atm 2/1
[local]Redback(config-atm-oc)#atm pvc 0 32 profile dslam1 encapsulation bridge1483
[local]Redback(config-atm-pvc)#
```

The following example shows how to configure a static PVC on an ATM OC port, encapsulates it with `ppp` mode, and specifies the auto-detect feature:

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-oc)#atm pvc 0 32 profile ubr encapsulation ppp auto
[local]Redback(config-atm-pvc)#
```

The following example shows how to configure a static PVC on an ATM OC port and encapsulates it with `raw` mode:

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-oc)#atm pvc 0 32 profile ubr encapsulation raw
[local]Redback(config-atm-pvc)#
```

The following example shows how to create a range of `32` static PVCs on a single VP on an ATM OC port; all PVCs use the ATM profile, `bdg`, and `bridge1483` encapsulation:

```
[local]Redback(config)#port atm 3/2
[local]Redback(config-atm-oc)#atm pvc explicit 10:32 through 10:63 prof bdg encaps bridge1483
[local]Redback(config-atm-pvc)#
```

The following example shows how to create a range of `32` on-demand PVCs on a single VP on an ATM OC port; all PVCs use the ATM profile, `bdg`, and `pppoe` encapsulation:

```
[local]Redback(config)#port atm 3/3
[local]Redback(config-atm-oc)#atm pvc on-demand 10:32 through 10:63 prof bdg encaps pppoe


Port:Channel 12/1 :1       VPI: 20   VCI: 32     Profile: ubr
Description:
Status: Down  Counters:   L2  Encapsulation:      multi
Bound to: ---
QoS - outbound ATMWFQ policy: (None Specified)
Circuit Range: yes      CCOD: no
First Created: Wed Oct  5 20:59:31 2005
Status Change: Wed Oct  5 20:59:31 2005
OAM Cross Connect   : Disabled
OAM Managed         : Disabled
OAM Fault Monitoring: Disabled

Port:Channel VPI VCI   VC HANDLE  State Encaps        Binding          Mode
12/1 :1      40  32    ---        Down  on-demand     no binding       dormant
active: 0        idle: 0        idle-down: 0
static: 0        wait: 0        dormant:   1
total: 1
```

```
[local]Redback#show atm pvc 12/1 all
```

1.18 atm scramble

For an ATM OC port in ATM OC configuration mode, the command syntax is:

atm scramble

no atm scramble

1.18.1 Purpose

Enables Asynchronous Transfer Mode (ATM) cell payload scrambling on an ATM OC port.

1.18.2 Command Mode

- ATM OC configuration

1.18.3 Syntax Description

This command has no keywords or arguments.

1.18.4 Default

ATM cell payload scrambling is enabled on the port.

1.18.5 Usage Guidelines

Use the **atm scramble** command on an ATM OC port to enable ATM cell payload scrambling as specified in section 4.5.3 in the *ITU-T I432* specification.

Note: Enabling or disabling ATM cell payload scrambling on an ATM port has no impact on the C2 byte, which is not included in the ATM cell payload; it is always set to 0x13.

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

1.18.6 Examples

The following example shows how to disable ATM cell payload scrambling on ATM port `1` of the ATM OC line card installed in slot `11`:

```
[local]Redback(config)#port atm 11/1
[local]Redback(config-atm-oc)#no atm scramble
```

The following example shows how to disable ATM cell payload scrambling on ATM port `1` of the ATM OC line card installed in slot `12`:

```
[local]Redback(config)#port atm 12/1

[local]Redback(config-atm-ds3)#no atm scramble
```

1.19 atm to qos

atm {*clp-value* | **all**} **to qos** *pd-value*

{**no** | **default**} **atm** {*clp-value* | **all**}

1.19.1 Purpose

Translates Asynchronous Transfer Mode (ATM) cell loss priority (CLP) values into packet descriptor (PD) quality of service (QoS) values on ingress.

1.19.2 Command Mode

Class map configuration

1.19.3 Syntax Description

clp-value	Either 0 or 1, representing the CLP bit in the ATM cell header. If a packet is composed of multiple ATM cells, the SmartEdge router considers the overall packet CLP value to be 1 if any ATM cell that makes up the AAL5 packet has the CLP bit set to 1 (for second-generation ATM line cards).
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
pd-value	An integer from 0 to 63 (six bits), with the packet priority encoded in three higher-order bits and the packet drop precedence in the three lower-order bits. You can enter the value in decimal or hexadecimal format, for example `16` or `0x10`. You can also enter a standard Differentiated Services Code Point (DSCP) marking label as defined in *DSCP Class Keywords* in the command *violate mark dscp*. The scale used by this command for packet priority, from 0 (lowest priority) to 7 (highest priority), is the relative inverse of the scale used by the **mark priority** command. For details on this command, see *Configuring Rate-Limiting and Class-Limiting*.

1.19.4 Default

ATM ingress classification maps use the CLP-to-PD mapping described in Table 4.

1.19.5 Usage Guidelines

Use the **atm to qos** command to translate ATM CLP values into PD QoS values on ingress.

If you specify the **all** keyword, all valid ATM CLP values are mapped to the specified QoS value. Any existing configuration for the classification map is overridden. You can use the **all** keyword to specify a single default value for both mapping entries, then override that value for a subset of entries by entering subsequent mapping commands without this keyword.

Use the **no** or **default** form of this command to revert one or both map entries to the default mapping described in Table 4.

Table 4 Default Mapping of ATM CLP Bits to QoS PD Values

ATM CLP	PD QoS Priority	PD Drop-Precedence	DSCP	PD QoS Code Point
0	1	2	AF11	10
1	0	0	DF	0

1.20 atm use-ethernet

atm {***clp-value*** | **all**} **use-ethernet** [***class-map-name***]

{**no** | **default**} **atm** {***clp-value*** | **all**}

1.20.1 Purpose

Determines initial packet descriptor (PD) values by mapping from the user priority bits in the 802.1p virtual LAN (VLAN) Tag Control Information (TCI) field of the packet header rather than directly from the Asynchronous Transfer Mode (ATM) cell loss priority (CLP) value for received ATM packets with the specified CLP value.

1.20.2 Command Mode

Class map configuration

1.20.3 Syntax Description

clp-value	Either 0 or 1, representing the CLP bit in the ATM cell header. If a packet is composed of multiple ATM cells, the SmartEdge router considers the overall packet CLP value to be 1 if any ATM cell that makes up the AAL5 packet has the CLP bit set to 1 (for second-generation ATM line cards).
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
use-ethernet	Enables a secondary mapping lookup using the packet's Ethernet 802.1p bits as input. If no classification map is specified for the secondary lookup, the default 8P0D mapping is used.
class-map-name	Optional. Name of the secondary classification map.

1.20.4 Default

ATM ingress classification maps use the CLP-to-PD mapping described in Table 5.

1.20.5 Usage Guidelines

Use the **atm use-ethernet** command to determine initial PD values by mapping from the user priority bits in the 802.1p VLAN TCI field of the packet header rather than directly from the ATM CLP value for received ATM packets with the specified CLP value.

If a packet includes both an outer permanent virtual circuit (PVC) header and an outer PVC Ethernet type field value of 0x8100 or 0x88a8, the inner PVC 802.1p header determines the PD value. If a packet does not include an Ethernet VLAN header, the SmartEdge router uses the default mapping described in Table 5.

Only packets with an outer PVC Ethernet type field value of 0x8100 or 0x88a8 are examined for enclosed inner PVC 802.1p values. The SmartEdge router uses the outer PVC 802.1p value to map all other outer PVC Ethernet types.

If you specify the **all** keyword, both CLP value entries are mapped to the specified PD value. Any existing configuration for the classification map is overridden. You can use the **all** keyword to specify a single default value for both mapping entries, then override that value for an entry by entering a subsequent mapping command without this keyword.

If you specify the ***class-map-name*** argument, the resulting mapping uses the specified 802.1p-to-PD classification map. The secondary classification map must have a value of ethernet for the ***marking-type*** argument and a value of in for the mapping direction. If you do not specify a secondary classification map, the SmartEdge router uses the default 8P0D mapping.

Use the **no** or **default** form of this command to revert one or both map entries to the default mapping described in Table 5.

Table 5 Default Mapping of ATM CLP Bits to QoS PD Values

ATM CLP	PD QoS Priority	PD Drop-Precedence	DSCP	PD QoS Code Point
0	1	2	AF11	10
1	0	0	DF	0

1.21 atm use-ip

atm {***clp-value*** | **all**} [***class-map-name***]

{**no** | **default**} **atm** {***clp-value*** | **all**}

1.21.1 Purpose

Determines initial packet descriptor (PD) values by mapping from the Differentiated Services Code Point (DSCP) value in the IP packet header rather than Ethernet 802.1p values on ingress for received Asynchronous Transfer Mode (ATM) packets with the specified cell loss priority (CLP) value.

1.21.2 Command Mode

Class map configuration

1.21.3 Syntax Description

clp-value	Either 0 or 1, representing the CLP bit in the ATM cell header. If a packet is composed of multiple ATM cells, the SmartEdge router considers the overall packet CLP value to be 1 if any ATM cell that makes up the AAL5 packet has the CLP bit set to 1 (for second-generation ATM line cards).
all	Maps all valid values for the source value to the specified target value. Any existing configuration for the classification map is overridden.
use-ip	Enables a secondary mapping lookup using the packet's DSCP bits as input. If no classification map is specified for the secondary lookup, the default DSCP-to-target mapping is used.
class-map-name	Optional. Name of the secondary classification map.

1.21.4 Default

ATM ingress classification maps use the CLP-to-PD mapping described in Table 6.

1.21.5 Usage Guidelines

Use the **atm use-ip** command to determine initial PD values by mapping from the DSCP value in the IP packet header rather than Ethernet 802.1p values on ingress for received ATM packets with the specified CLP value. If a packet does not include an IP header, the SmartEdge router uses the default mapping described in Table 6.

Only 802.1p packets with an outer PVC Ethernet type field value of 0x8100 or 0x88a8 are examined for DSCP values in the packet header. The SmartEdge router uses the default mapping described in Table 6 for packets with all other VLAN Ethernet types.

If you specify the **all** keyword, both PD bits are set to the specified CLP value. Any existing configuration for the classification map is overridden. You can use the **all** keyword to specify a single default value for both mapping entries, then override that value for an entry by entering a subsequent mapping command without this keyword.

If you specify the ***class-map-name*** argument, the resulting mapping uses the specified DSCP-to-PD classification map. The secondary classification map must have a value of ip for the ***marking-type*** argument and a value of in for the mapping direction. If you do not specify a secondary classification map, the SmartEdge router copies the DSCP value directly to the internal QoS PD value.

Use the **no** or **default** form of this command to revert one or both map entries to the default described in Table 6.

Table 6 Default Mapping of ATM CLP Bits to QoS PD Values

ATM CLP	PD QoS Priority	PD Drop-Precedence	DSCPI	PD QoS Code Point
0	1	2	AF11	10
1	0	0	DF	0

1.22 atm vp

atm vp ***vpi*** **profile** ***prof-name***

no atm vp ***vpi*** **profile**

1.22.1 Purpose

Creates or modifies a shaped virtual path (VP) on an ATM OC port.

1.22.2 Command Mode

- ATM OC configuration

1.22.3 Syntax Description

vpi	Virtual path identifier (VPI). The range of values is 0 to 255.
profile ***prof-name***	Profile to use for the VP.

1.22.4 Default

No VPs are defined.

1.22.5 Usage Guidelines

Use the **atm vp** command to create or modify a shaped VP on an ATM OC port.

When you create an ATM permanent virtual circuit (PVC), you must specify a VP for it, using a VPI. An ATM VP can be shaped or nonshaped:

- Shaped VP—Is associated with an ATM profile.
- Nonshaped VP— Has no profile associated with it.

The SmartEdge router creates a nonshaped VP when you configure an ATM PVC and specify a VPI that has not be used to create a shaped VP. To create a shaped VP, you must create it explicitly using this command.

You cannot convert a nonshaped VP to a shaped VP unless and until you delete all the PVCs that reference it. Deleting all the PVCs that reference it effectively deletes the nonshaped VP.

Note: Hierarchical-shaped virtual circuits (HSVCs), by definition, always use a shaped VP.

The only modification possible for a shaped VP is to specify a different profile. To modify a shaped VP, enter this command with the name of the new profile. If the shaped VP has PVCs configured on it, the current and new profiles must specify the same traffic class; otherwise, the system displays an error message. You must then delete the PVCs or HSVCs on the shaped VP before specifying the new profile and recreate them afterwards.

Note: For more configuration guidelines for ATM profiles, VPs, and PVCs, see *ATM Configuration Guidelines* in *Configuring Circuits*.

Use the **no** form of this command to delete a shaped VP.

Note: If a shaped VP is deleted, all associated PVCs or HSVCs are deleted from the configuration.

1.22.6 Examples

The following example shows how to create a shaped VP on an ATM OC port and references a profile, `cbr-profile`:

```
[local]Redback(config-atm-oc)#atm vp 20 profile cbr-profile
```

1.23 attached-bit

attached-bit {**ignore** | **never-set**}

no attached-bit {**ignore** | **never-set**}

1.23.1 Purpose

Configures the Intermediate System-to-Intermediate System (IS-IS) attached bit preferences in level 1 (L1) link-state protocol data units (LSPs).

1.23.2 Command Mode

IS-IS router configuration

1.23.3 Syntax Description

ignore	Configures IS-IS L1 routing to ignore the attached bit in LSPs. The IS-IS L1 router does not install a default route towards level 2 (L2) gateways.
never-set	Configures the IS-IS router to not set the attached bit in its L1 LSP, even if it is L2 attached.

1.23.4 Default

The ignore and never set preferences are both disabled.

1.23.5 Usage Guidelines

Use the **attached-bit** command to configure the IS-IS attached bit preferences in L1 LSPs.

Routers in an IS-IS L1 area exchange information within the L1 area. For IP destinations not found in the prefixes in the L1 database, the L1 router must forward packets to the nearest router that is in both IS-IS L1 and L2 with the attached bit set in its L1 LSP.

Use the **ignore** keyword on an IS-IS L1 router when route leaking is enabled on the IS-IS L2 gateways. When the **ignore** keyword is specified, the router ignores the attached bit on incoming L1 LSPs, and no default route is installed for the router that has the attached bit set in its LSP.

Use the **never-set** keyword on an L1L2 router when route leaking is enabled on the router. When the **never-set** keyword is specified, the router does not set the attached bit in its L1 LSP.

Use the **no** form of this command to disable a configured attached bit preference. You must include either the **ignore** or **never-set** keyword to disable each preference separately.

1.23.6 Examples

The following example shows how to configure an L1 router to ignore the attached bits from incoming L1 LSPs:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#attached-bit ignore
```

1.24 attribute

In RADIUS policy configuration mode, the syntax is:

attribute [**vendor-specific** {**rbak** | *vendor-num*}] {*attribute-name* | *attribute-num*} **drop** [*msg-type-1*... *msg-type-n*]

{**no** | **default**} **attribute** [**vendor-specific** {**rbak** | *vendor-num*}] *attribute-num*

In parameter-array-loop configuration and service policy configuration mode, the syntax is:

[**seq** *seq-num*] **attribute** *attribute-name* {**in** | **out**} {*attribute-value* | *$param-list-name*}

no seq *seq-num*

1.24.1 Purpose

In RADIUS policy configuration mode, specifies one or more Remote Authentication Dial-In User Service (RADIUS) messages in which the specified attribute is to be dropped. In service policy configuration mode, specifies the attribute for a dynamic service condition in which one or more fields are defined.

1.24.2 Command Mode

- Parameter array loop configuration
- RADIUS policy configuration
- Service policy configuration

1.24.3 Syntax Description

In RADIUS policy configuration mode, the keywords and arguments are:

vendor-specific	Optional. Specifies a vendor-specific attribute (VSA) instead of a RADIUS standard attribute.
rbak	Specifies that the attribute is a vendor VSA provided by Ericsson AB. Required only if you enter the **vendor-specific** keyword.
vendor-num	Specifies that the attribute is a VSA of another vendor. Required only if you enter the **vendor-specific** keyword.
attribute-name	RADIUS attribute or VSA name. For the supported RADIUS standard attributes and vendor VSAs provided by Ericsson AB, see *RADIUS Attributes*. For the keywords to use for these RADIUS standard attributes and vendor VSAs provided by Ericsson AB, see the online Help in the command-line interface (CLI).
attribute-num	RADIUS attribute or VSA number. For the numbers of supported RADIUS standard attributes and vendor VSAs provided by Ericsson AB, see *RADIUS Attributes*.
drop	Specifies one or more attributes to be dropped. Not entered in the **no** form.
msg-type-1 ... msg-type-n	Optional. One or more of the following RADIUS message types in which the attribute is to be removed: • **access-accept**—Access-Accept message. • **access-request**—Access-Request message. • **acct-start**— Accounting-Start message. • **acct-stop**—Accounting-Stop message. • **acct-update**—Accounting-Update message. • **coa-request**—Change-of-Authority message. • **service-acct-stop**— Service Accounting-Stop message. • **service-acct-start**— Service Accounting-Start message. • **service-acct-update**— Service Accounting-Update message. If you do not specify a message type, the attribute is dropped from all RADIUS messages.

In parameter array loop configuration or service policy configuration mode, the keywords and arguments are:

seq ***seq-num***	Optional. Sequence number for the statement. The range of values is 1 to 1,000.
attribute-name	Name of the attribute, according to one of the keywords listed in Table 7.

in	Required for certain attributes; see Table 7. Applies the attribute to incoming traffic.
out	Required for certain attributes; see Table 7. Applies the attribute to outgoing traffic.
attribute-value	String defining the fields within the attribute, enclosed in quotation marks (“ ”), according to the format for the attribute.
param-list-name	Name of an array that defines a list of values for a field within the attribute.

1.24.4 Default

In RADIUS policy configuration mode, this RADIUS attribute or the VSA is not dropped from any RADIUS message from which it appears. There is no default in parameter array loop or service policy configuration mode.

1.24.5 Usage Guidelines

In RADIUS policy configuration mode, use the **attribute** command to specify one or more RADIUS messages in which the specified attribute is to be dropped.

You can specify the attribute using either the ***attribute-name*** or ***attribute-num*** argument. If the attribute name is listed in *RADIUS Attributes*, but not in the online help for the CLI, enter the attribute number.

Note: The online help for the CLI includes all RADIUS standard attributes and vendor VSAs provided by Ericsson AB, some of which are not supported by the SmartEdge router.

You can specify any or all message types, separated by spaces, in a single instance of the command, or you can enter them individually.

Use the **no** or **default** form of this command to restore this RADIUS attribute or VSA to any RADIUS message in which it appears.

In parameter array loop or service policy configuration mode, use the **attribute** command to specify the RADIUS standard attribute, vendor VSA provided by Ericsson AB, or service attribute for a dynamic service condition in which one or more fields are defined. Table 7 lists the possible values for the ***attribute-name*** argument and the service condition it supports. For attribute format descriptions, see the following tables in *RADIUS Attributes*:

- RADIUS standard attributes—*Supported Standard RADIUS Attributes*
- Vendor VSAs provided by Ericsson AB—*Vendor VSAs*
- Other VSAs—*Other Supported VSAs*

- Service attributes—*Supported Service Attributes*

Table 7 Service Condition Keywords for the attribute-name Argument

Service Condition	Attribute Name	Attribute #	Notes
Dynamic ACLs	**Ascend-Data-Filter**	242	
Dynamic policy ACLs	**Dynamic-Policy-Filter**	VSA 164	
Dynamic QoS policy options	**Dynamic-QoS-Parameter**	VSA 196	
Dynamic traffic filtering	**Filter-Id**	RADIUS 11	Use the **in** and **out** keywords as appropriate.
Forward policy	**Forward-Policy**	VSA 92	Use the **in** and **out** keywords as appropriate.
HTTP redirect	**HTTP-Redirect-Profile-Name**	VSA 107	
HTTP redirect	**HTTP-Redirect-URL**	VSA 165	
IGMP service profile	**IGMP-Service-Profile**	VSA 90	
Interim accounting interval	**Service-Interim-Accounting**	–	
Metering policy	**Qos-Metering**	VSA 88	
NAT policy	**NAT-Policy**	VSA 105	
Policing policy	**Qos-Policing**	VSA 87	
PWFQ policy	**Qos-Queuing**	VSA 89	
QoS-Rate-Inbound	**Qos-Rate**	VSA 156	Use the **in** keyword.
QoS-Rate-Outbound	**Qos-Rate**	VSA 157	Use the **out** keyword.
Service timeout limit	**Service-Timeout**	–	
Service volume limit	**Service-Volume-Limit**	–	

You use this command to specify one or more fields in an attribute that has a single value; if a field can have multiple values, enter the **foreach** command (in service profile configuration mode) with the name of the field that supports multiple values, followed by the **attribute** command that includes that field. For more information about using the **attribute** command for fields with multiple values, see the *foreach* command description.

Note: Only the Ascend-Data-Filter, Dynamic-Policy-Filter, and Dynamic-QoS-Parameter attributes support fields with multiple values.

You must enter this command for each service attribute that includes one or more fields for which you have created an entry using the **parameter** command (in service profile configuration mode). The maximum number of attribute instances in a service profile is 32; an attribute instance is each occurrence of the command in service profile configuration mode plus each instance in a **foreach** loop (in parameter array loop configuration mode) for each parameter value.

For example, if a service profile includes two attributes each with two fields with a single parameter value and one attribute with a field with a parameter list with four values, that service profile has six attribute instances.

You can use the optional **seq** ***seq-num*** construct with the **attribute** command to establish a sequence number for the statement you are creating. If you do not use the **seq** ***seq-num*** construct, the system automatically assigns sequence numbers to the statements that you enter, in increments of 10. The first statement that you enter is assigned the sequence number 10, the second is assigned the number 20, and so on. This allows room to assign intermediate sequence numbers to statements that you might want to add later. In the parameter-array-loop or service policy configuration mode, use the **no** form of this command along with the specified sequence number to remove the attribute statement from the service profile.

1.24.6 Examples

The following example shows how to create the `custom` RADIUS policy to drop RADIUS attribute `123` in all RADIUS messages and vendor VSA provided by Ericsson AB`10` in Access-Request messages:

```
[local]Redback(config)#radius policy name custom
[local]Redback(config-rad-policy)#attribute 123 drop
[local]Redback(config-rad-policy)#attribute rbak 10 drop access-request
```

The following example specifies the `HTTP-Redirect-URL` attribute to define a dynamic URL:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius service profile redirect
[local]Redback(config-svc-profile)#parameter value redirect-url
[local]Redback(config-svc-profile)#attribute HTTP-Redirect "$redirect-url"
```

The following example specifies the `Dynamic-Policy-Filter` attribute for multiple TCP ports within a **foreach** loop.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius service profile redirect
[local]Redback(config-svc-profile)#parameter list tcp-port
[local]Redback(config-svc-profile)#foreach tcp-port
[local]Redback(config-param-array-loop)#attribute Dynamic-Policy-Filter "ip in forward tcp
 dstport = $tcp-port class redirect forward"
```

1.25 attribute (RSVP)

attribute ***name value***

no attribute ***name value***

1.25.1 Purpose

Configures Resource Reservation Protocol traffic engineering (RSVP-TE) link attributes for Constrained Shortest Path First (CSPF).

1.25.2 Command Mode

RSVP link attribute configuration

1.25.3 Syntax Description

name	Specifies an RSVP link attribute. The RSVP link attribute name is typically a color.
value	Number from 0 to 31 that is associated with an administrative group.

1.25.4 Default

No link attributes are defined.

1.25.5 Usage Guidelines

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

You can use the administrative group as part of a constraint (using the **admin-group** command in RSVP constraint configuration mode), or you can use it to define the administrative group that the interface belongs to (in interface configuration mode).

Use the **no** form of this command to delete a link attribute.

1.25.6 Examples

The following example shows how to specify a link attribute with the name `red` that is a member of administrative group 2:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#link-attributes
[local]Redback(config-rsvp-link-attr)#attribute red 2
```

1.26 au3

au3 ***au-num***

1.26.1 Purpose

Selects an administrative unit-3 (AU-3) on a channelized port and enters AU-3 configuration mode.

1.26.2 Command Mode

STM-1 configuration

STM-4 configuration

1.26.3 Syntax Description

au-num	AU number. The range of values is 1 to 3.

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **au3** command to specify that AU-3 administrative units will be mapped into the AUG-1 administrative unit groups.

1.26.6 Examples

The following example shows how to select an AU-3 on a channelized port:

```
[local]Redback(config-stm1)#au3 3
[local]Redback(config-au3)#
```

1.27 au4

au4 ***au-num***

1.27.1 Purpose

Selects an administrative unit-4 (AU-4) on a channelized port and enters AU-4 configuration mode.

1.27.2 Command Mode

STM-1 configuration

STM-4 configuration

1.27.3 Syntax Description

au-num	AU number. The range of values is 1 to 3.

1.27.4 Default

None

1.27.5 Usage Guidelines

Use the **au4** command to specify that AU-4 administrative units will be mapped into the AUG-1 administrative unit groups.

1.27.6 Examples

The following example shows how to select an AU-4 on a channelized port:

```
[local]Redback(config-stm1)#au4 3
[local]Redback(config-au3)#
```

1.28 aug-mapping

aug-mapping ***mapping-specification***

{no | default}aug-mapping

1.28.1 Purpose

Configures the current SDH port for au3-no-tug, au3-tu11, au3-tu12, au4-tu3, au4-tu11, or au4-tu12 mapping.

1.28.2 Command Mode

STM-1 configuration

STM-4 configuration

1.28.3 Syntax Description

mapping-specification	• **au3-no-tug** Specifies that AU-3 administrative units are mapped into the AUG-1 administrative unit groups and that no TUGs map into the AU, and therefore no TUs are mapped into TUGs. This option is only valid when the port AUG mapping is set to AU-3 and is required to carry each DS3 channel within a VC3 on the AU-3. • **au3-tu11** Specifies that AU-3 administrative units are mapped into the AUG-1 administrative unit groups and that TU-11 units map into TUG-2s. This mapping is required to carry each DS1 channel on an SDH port. • **au3-tu12** Specifies that AU-3 administrative units are mapped into the AUG-1 administrative unit groups and that TU-12 units map into TUG-2s. This mapping is required to carry each E1 channel on an SDH port. • **au4-tu3** Specifies that AU-4 administrative units are mapped into the AUG-1 administrative unit groups and that TU-3 units map into TUG-3s. This mapping is required to carry each DS3 channel on an SDH port, where AUG mapping is set to AU-4. • **au4-tu11** Specifies that AU-4 administrative units are mapped into the AUG-1 administrative unit groups and that TU-11 units map into TUG-2s. This mapping is required to carry each DS1 channel on an SDH port. • **au4-tu12** (default) Specifies that AU-4 administrative units are mapped into the AUG-1 administrative unit groups and that TU-12 units map into TUG-2s. This mapping is required to carry each E1 channel on an SDH port.

1.28.4 Default

au-4-tu-12

1.28.5 Usage Guidelines

1.28.5.1 Where Used

The **aug-mapping** command plays an important role in the provisioning of channelized STM-1 and STM-4 ports. For channel-mapping of channelized OC-3 and OC-12 ports, see the *channel-mapping* command. For detailed examples, the supported subchannel types, and the full context of this command, see *Configuring Channelized Ports*.

1.28.5.2 Usage

The port SDH mapping specifies the AUG mapping used by all facilities on the current SDH port. The AUG mapping selected must match that of the far-end SDH interface, and must support the types of channels required to carry the POS or CES service.

- The port mapping limits the channel type that can be carried by the port.
- All configured channels must be removed from the port before its port mapping can be changed.
- Table 8 shows the service provided on each type of unchannelized channel with each SDH mapping option. Table 8 also shows what subchannel channel types can be multiplexed on each channelized channel type for each SDH mapping option.

Table 8 Channel Types

Channel Type	Subchannel/ Service Type	Framing	SONET Channel Mapping	SDH AUG Mapping
DS3	POS	C-Bit parity M23	STS1	au3/no-tugs au4/tu3
channelized DS3	DS1 E1	C-Bit parity M23	STS1	au3/no-tugs au4/tu3
DS1	POS	SF ESF	VT1.5	au3/tu11 au4/tu11
channelized DS1	NxDS0	SF ESF	VT1.5	au3/tu11 au4/tu11

E1	POS	CRC-4 NO-CRC-4 unframed	N/A	au3/tu12 au4/tu12
Channelized E1	NxDS0	CRC-4 NO-CRC-4	N/A	au3/tu12 au4/tu12

Note: Because SDH and SONET mappings are applied on a per-port basis, channels that require different SDH or SONET mappings are not supported on the same port.

1.28.6 Examples

This example illustrates the use of **`au4-tu12`** aug-mapping in the multiplexing of E1 channels from a channelized STM-1 port:

```
config
!
service multiple-contexts
!
software license
 all-ports password <plain text passcode> card ch-oc3oc12-8or2-port slot 2
!
!
card ch-oc3oc12-8or2-port 2
 no shutdown
 clock-source global-reference
!
!
! Example for POS, using SDH AUG mapping au4-tu12 to channelize:
! chSTM1 -> E1
! chSTM1 -> chE1 -> DS0s
!
port channelized-stm1 2/4 pos
 no shutdown
 aug-mapping au4-tu12
 clock-source card-reference
 !
 port e1 2/4:1
  no shutdown
  clock-source card-reference
  encapsulation ppp
  bind interface pos_chstm1->e1_1 redkite1
 !
 port e1 2/4:2
  no shutdown
  clock-source card-reference
  encapsulation ppp
  bind interface pos_chstm1->e1_2 redkite1
 !
 port channelized-e1 2/4:3
  no shutdown
  clock-source card-reference
 !
  port ds0s 2/4:3:1
   no shutdown
   timeslot 1-30
   encapsulation ppp
   bind interface pos_chstm1->che1->ds0s_1 redkite1
  !
  port ds0s 2/4:3:31
   no shutdown
   bind interface pos_chstm1->che1->ds0s_2 redkite1
  !
 !
!
!
end
```

1.29 authentication foreign-agent

```
authentication foreign-agent hmac-md5 {key-chain-name |
dynamic-key wimax}

no authentication foreign-agent
```

1.29.1 Purpose

Configures authentication between this HA instance and its FA peers.

1.29.2 Command Mode

HA configuration

1.29.3 Syntax Description

hmac-md5	Specifies the Hash-based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm.
key-chain-name	Name of an existing key chain that you must have configured in the context in which you have configured the HA instance.
dynamic-key wimax	Specifies to use the Motorola FA-HA key Vendor Specific Attribute (VSA) for FA-HA authentication. The Motorola FA-HA-Key VSA ID is 26/161/67. The Motorola WiMax solution provides this VSA to the FA. For more information about supported WiMax Attributes, see *Motorola VSAs for Mobile IP Supported by the SmartEdge Router* in *RADIUS Attributes*.

1.29.4 Default

No authentication is configured for the HA instance or its FA peers.

1.29.5 Usage Guidelines

Use the **authentication foreign-agent** command to configure authentication between this HA instance and its FA peers.

In HA configuration mode, this command configures the default authentication between the HA and its FA peers.

Use the **no** form of this command to remove the authentication configuration for this HA instance and its FA peers.

1.29.6 Examples

The following example shows how to configure the `key-ha` key chain for key`100` and an security parameter index (SPI) of `256` for incoming traffic and then specify it when configuring the default authentication between an HA instance and its FA peers:

```
[local]Redback(config)#context ha
[local]Redback(config-ctx)#key-chain key-ha key-id 100
[local]Redback(config-key-chain)#spi 256
[local]Redback(config-key-chain)#key-string hex 0xfeedaceedeadbeef
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#context ha
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#home-agent
[local]Redback(config-mib-ha)#authentication foreign-agent hmac-md5 key-ha
```

The following example shows how to configure dynamic keys between an HA instance and its FA peers:

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

[local]Redback(config-ctx)#router mobile-ip

[local]Redback(config-mip)#home-agent

[local]Redback(config-mib-ha)#authentication foreign-agent hmac-md5 dynamic-key wimax
```

1.30 authentication (home agent peer instance)

authentication {none | hmac-md5 {*key-chain-name* | dynamic-key wimax proprietary}

no authentication

1.30.1 Purpose

Configures authentication between this FA instance and a specific HA peer.

1.30.2 Command Mode

HA peer configuration

1.30.3 Syntax Description

hmac-md5	Specifies the Hash-based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm.
key-chain-name	Name of an existing key chain, which you must have configured in the context in which you have configured the HA peer.
dynamic-key wimax	Specifies to use the Motorola FA-HA key Vendor Specific Attribute (VSA) for FA-HA authentication. The Motorola FA-HA-Key VSA ID is 26/161/67. The Motorola WiMax solution provides this VSA to the FA. For more information about supported WiMax Attributes, see *Motorola VSAs for Mobile IP Supported by the SmartEdge Router* in *RADIUS Attributes*.

1.30.4 Default

No authentication is configured for any FA instance or HA peer.

1.30.5 Usage Guidelines

Use the **authentication** command to configure authentication between this FA instance and a specific HA peer.

Use the **no** form of this command to remove the authentication configuration for this FA instance or HA peer.

1.30.6 Examples

The following example shows how to configure dynamic keys between the FA instance and a specific HA peer:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip)#home-agent-peer 1.1.1.1
[local]Redback(config-mip-fa)#authentication hmac-md5 dynamic-key wimax proprietary
```

1.31 authentication home-agent

authentication home-agent hmac-md5 {***key-chain-name*** | **dynamic-key wimax**}

no authentication home-agent

1.31.1 Purpose

Configures authentication between this FA instance and its HA peers.

1.31.2 Command Mode

FA configuration

1.31.3 Syntax Description

hmac-md5	Specifies the Hash-based Message Authentication Code (HMAC)- Message Digest 5 (MD5) algorithm.
key-chain-name	Name of an existing key chain that you must have configured in the context in which you have configured the FA instance or HA peer.
dynamic-key wimax	Specifies to dynamically compute FA-HA keys using the WiMAX AAA HA-RK-Key Vendor Specific Attribute (VSA). The WiMAX HA-RK-Key VSA ID is 26/24757/15. Configured static key chains take precedence over dynamic keys. For more information about supported WiMax Attributes, see *RADIUS Attributes Supported by Mobile IP Services* in *RADIUS Attributes*.

1.31.4 Default

No authentication is configured for any FA instance or HA peers.

1.31.5 Usage Guidelines

Use the **authentication home-agent** command to configure authentication between this FA instance and its HA peers.

In FA configuration mode, this command configures the default authentication between the HA instance and its FA peers.

Use the **no** form of this command to remove the authentication configuration for this HA instance.

1.31.6 Examples

The following example shows how to configure the `key-ha` key chain for key `100` and an security parameter index (SPI) of `256` for incoming traffic and then

specifies it when configuring the default authentication between an FA instance and its HA peers:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#key-chain key-ha key-id 100
[local]Redback(config-key-chain)#spi 256
[local]Redback(config-key-chain)#key-string hex 0xfeedaceedeadbeef
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#authentication home-agent hmac-md5 key-ha
```

The following example shows how to configure dynamic keys between an FA instance and its HA peers:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#authentication home-agent hmac-md5
dynamic-keys wimax proprietary
```

1.32 authentication (foreign agent peer instance)

authentication {**none** | **hmac-md5** {***key-chain-name*** | **dynamic-key wimax** }

no authentication

1.32.1 Purpose

Configures authentication between this HA instance and a specific FA peer.

1.32.2 Command Mode

FA peer configuration

1.32.3 Syntax Description

hmac-md5	Specifies the Hash-based Message Authentication Code (HMAC)- Message Digest 5 (MD5) algorithm.
key-chain-name	Name of an existing key chain, which you must have configured in the context in which you have configured the HA instance or FA peer.
dynamic-key wimax	Specifies to dynamically compute FA-HA keys using the WiMAX AAA HA-RK-Key Vendor Specific Attribute (VSA). The WiMAX HA-RK-Key VSA ID is 26/24757/15. Configured static key chains take precedence over dynamic keys. For more information about supported WiMax Attributes, see *RADIUS Attributes Supported by Mobile IP Services* in *RADIUS Attributes*.

1.32.4 Default

No authentication is configured for any HA instance or FA peer.

1.32.5 Usage Guidelines

Use the **authentication** command to configure authentication between this HA instance and a specific FA peer.

Use the **no** form of this command to remove the authentication configuration for the FA peer.

1.32.6 Examples

The following example shows how to configure dynamic keys between the HA instance and a specific FA peer:

```
[local]Redback(config)#context ha
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#home-agent
[local]Redback(config-mip)#foreign-agent-peer 1.1.1.1
[local]Redback(config-mib-ha)#authentication hmac-md5 dynamic-key wimax
```

1.33 authentication (IS-IS)

authentication [**level-1** | **level-2**] **key-chain** ***key-chain-name*** [**type** {**hmac-md5** | **simple**}] [**lsp-only**] [**no-check**]

no authentication {**level-1** | **level-2**} **key-chain** ***key-chain-name*** [**type** {**hmac-md5** | **simple**}] [**lsp-only**] [**no-check**]

1.33.1 Purpose

Configures Intermediate System-to-Intermediate System (IS-IS) routing packet authentication using the simple or Hash-Based Message Authentication Code-Message Digest 5 (HMAC-MD5) authentication scheme for the IS-IS interface or IS-IS instance.

1.33.2 Command Mode

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

1.33.3 Syntax Description

level-1	Optional, except in the **no** form of this command. Sets authentication for level 1 routing.
level-2	Optional, except in the **no** form of this command. Sets authentication for level 2 routing.
key-chain ***key-chain-name***	Name of the key chain used for authentication.
type	Optional. Specifies that a type of authentication follows.
hmac-md5	Specifies HMAC-MD5 authentication.
simple	Specifies simple authentication.
lsp-only	Optional. If specified, only IS-IS link-state protocol data units (LSPs) are authenticated. Otherwise, IS-IS Hello (IIH), partial sequence number protocol data units (PSNPs), complete sequence number protocol data units (CSNPs), and LSPs are authenticated.
no-check	Optional. Causes the SmartEdge router to use authentication when sending packets, but not to check the packets it receives. This function is used during the transition period so that both devices can turn on authentication without a flag day.

1.33.4 Default

Authentication is not enabled. When you enter this command without specifying either level 1 or level 2 routing, authentication is set for both levels of IS-IS routing. If no authentication type is specified, HMAC-MD5 is used.

1.33.5 Usage Guidelines

Use the **authentication** command in IS-IS interface configuration mode to configure IS-IS routing packet authentication using the simple or HMAC-MD5 authentication scheme for an IS-IS interface.

Use the **authentication** command in IS-IS router configuration mode to configure IS-IS routing packet authentication using the simple or HMAC-MD5 authentication scheme for an IS-IS instance. To use a different key for a specific interface, use the **authentication** command in IS-IS interface configuration mode.

IS-IS authentication increases the network routing security. This command authenticates all IS-IS packets on the IS-IS interface or IS-IS instance.

The **key-chain** ***key-chain-name*** construct is provided because a key chain is required for simple and MD5 authentication schemes. A key chain provides a method for centrally managing keys and supports automatic key rollover. For information on the **key-chain key-id** command, see *Configuring Key Chains*.

Caution!

Risk of insecure IS-IS authentication. Careful planning is necessary to ensure a smooth rollout of IS-IS authentication across a network. To reduce the risk, and because HMAC-MD5 is highly secure, we strongly recommend using a secure channel to configure the passwords.

Use the **no** form of this command to disable authentication. In the **no** form, you must include either the **level-1** keyword, the **level-2** keyword, or the **key-chain** ***key-chain-name*** construct.

1.33.6 Examples

The following example shows how to apply key chain, `key06`, to the IS-IS interface, `fa4/1`, using `simple` authentication:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#authentication key-chain key06 type simpl
```

The following example shows how to apply key chain, `key06`, to the IS-IS instance, `isis01`, using `HMAC-MD5` authentication:

```
[local]Redback(config-ctx)#router isis isis01
[local]Redback(config-isis)#authentication key-chain key06 type hmac-md5
```

1.34 authentication (local PAP, CHAP)

authentication {**pap** | **chap** | **pap chap** | **chap pap**} **username** ***name*** **password** ***password*** [**passive**]

no authentication {**pap** | **chap** | **pap chap** | **chap pap**} **username** ***name*** **password** ***password*** [**passive**]

1.34.1 Purpose

Enables PAP, CHAP, PAP-CHAP, or CHAP-PAP local authentication of static links.

1.34.2 Command Mode

- Link group configuration - Multilink Point-to-Point Protocol (MLPPP) link groups only

1.34.3 Syntax Description

pap	Use local PAP authentication.
chap	Use local CHAP authentication.
username ***name***	The name of the client to be authenticated.
password ***password***	The password of the client to be authenticated.
passive	Disables the SmartEdge router from initiating PPP authentication.

1.34.4 Default

Local authentication of static links is not enabled.

1.34.5 Usage Guidelines

Use the **authentication (local PAP, CHAP)** command to enable PAP, CHAP, PAP-CHAP, or CHAP-PAP local authentication of static links.

This command affects only local authentication, and does not apply to or change RADIUS authentication.

This command is supported only on single static PPP links and MLPPP link groups.

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

1.34.6 Examples

The following example illustrates the CHAP PAP option of this command for an MLPPP link group. The DS-1 channels in the **LG-abc** link group must be configured with PPP encapsulation:

```
 link-group LG-abc mp
  bind interface test1 test
  authentication chap pap username fred password flintstone passive
!
 port ds1 10/2:2
  no shutdown
  encapsulation ppp
  link-group LG-abc
```

The following example illustrates the CHAP option of this command for static PVC in a DS-1 channel:

```
 port ds1 10/2:1
  no shutdown
  encapsulation ppp
  authentication chap username alaska password pwd1
  bind interface xyz1 xyz
```

1.35 authentication mobile-node

authentication mobile-node hmac-md5 {**optional**}

no authentication mobile-node

1.35.1 Purpose

Configures processing of a mobile node (MN) foreign agent (FA) authentication extension in registration requests (RRQs).

1.35.2 Command Mode

FA configuration

1.35.3 Syntax Description

hmac-md5	Specifies the Hash-based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm.
optional	Process a MN-FA authentication extension as optional.

1.35.4 Default

Ignore MN-FA authentication extension.

1.35.5 Usage Guidelines

Use the **authentication mobile-node** command to process an MN-FA authentication extension and reject any RRQs that do not include MN-FA authentication extension (making MN-FA authentication extension mandatory).

Use the **optional** keyword to process all RRQs with or without an MN-FA authentication extension.

Use the **no** form of this command to resume default behavior and ignore any MN-FA authentication extension.

1.35.6 Examples

The following example shows how to configure the processing of MN-FA authentication extension as optional:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mib-ha)#authentication mobile-node hmac-md5 optional
```

The following example shows how to remove the processing of MN-FA extensions, resuming default behavior:

```
[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mib-ha)#no authentication mobile-node
```

1.36 authentication (OSPF)

authentication {**md5** ***key-chain-name*** | **none** | **simple** ***key-chain-name***}

{**no** | **default**} **authentication**

1.36.1 Purpose

Enables authentication and specifies the authentication scheme for the specified interface, sham link, or virtual link.

1.36.2 Command Mode

- OSPF interface configuration
- OSPF sham link configuration
- OSPF virtual link configuration

1.36.3 Syntax Description

md5 ***key-chain-name***	Message Digest 5 (MD5) authentication key chain name.
none	Specifies no authentication.
simple ***key-chain-name***	Simple authentication key chain name.

1.36.4 Default

Authentication is not enabled.

1.36.5 Usage Guidelines

Use the **authentication** command to enable authentication and specify the authentication scheme for the specified interface, sham link, or virtual link.

Key chains allow you to control authentication keys used by various routing protocols in the system. All routers connected to the same IP subnet must use the same authentication scheme and key ID. If multiple key IDs have been configured, the one with the most current send time is used. For information on the **key-chain key-id** command, see *Configuring Key Chains*.

Routes within the same area are not required to use the same authentication scheme and key ID. However, if two routers directly exchange updates, they must have the same authentication scheme and key ID.

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

1.36.6 Examples

The following example shows how to configure MD5 authentication for the interface, `193.4.5.2`, and simple authentication for the interface, `10.1.1.1`:

```
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#area 0.0.0.0
[local]Redback(config-ospf-area)#interface 193.4.5.2
[local]Redback(config-ospf-if)#authentication md5 auth01
[local]Redback(config-ospf-if)#exit
[local]Redback(config-ospf-area)#exit
[local]Redback(config-ospf)#area 0.0.0.1
[local]Redback(config-ospf-area)#interface 10.1.1.1
[local]Redback(config-ospf-if)#authentication simple auth02
[local]Redback(config-ospf-if)#exit
[local]Redback(config-ospf-area)#exit
[local]Redback(config-ospf)#exit
[local]Redback(config-ctx)#key-chain auth01 keyid 1
[local]Redback(config-key-chain)#key-string secret
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#key-chain auth02 keyid 1
[local]Redback(config-key-chain)#key-string password
```

1.37 authentication (RIP)

authentication {**md5** ***key-chain-name*** | **simple** ***key-chain-name***}

{**no** | **default**} **authentication**

1.37.1 Purpose

Enables authentication and specifies the authentication scheme for the Routing Information Protocol (RIP) interface.

1.37.2 Command Mode

RIP interface configuration

1.37.3 Syntax Description

md5 ***key-chain-name***	Message Digest 5 (MD5) authentication key chain name.
simple ***key-chain-name***	Simple authentication key chain name.

1.37.4 Default

Authentication is not enabled.

1.37.5 Usage Guidelines

Use the **authentication** command to enable authentication and specify the authentication scheme for the RIP interface.

Key chains allow you to control authentication keys used by various routing protocols in the system. All routers connected to the same IP subnet must use the same authentication scheme and key ID. If multiple key IDs have been configured, the one with the most current send time is used. For information on the **key-chain key-id** command, *Configuring Key Chains*.

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

1.37.6 Examples

The following example shows how to configure MD5 authentication for the RIP interface, `fe0`, and simple authentication for the RIP interface, `su12:`

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#interface fe0
[local]Redback(config-rip-if)#authentication md5 auth01
[local]Redback(config-rip-if)#exit
[local]Redback(config-rip)#interface su12
[local]Redback(config-rip-if)#authentication simple auth02
[local]Redback(config-rip-if)#exit
[local]Redback(config-rip)#exit
[local]Redback(config-ctx)#key-chain auth01 keyid 1
[local]Redback(config-key-chain)#key-string secret
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#key-chain auth02 keyid 1
[local]Redback(config-key-chain)#key-string password
```

1.38 authentication (RSVP)

authentication ***key-chain***

no authentication

1.38.1 Purpose

Enables authentication for a Resource Reservation Protocol (RSVP) interface.

1.38.2 Command Mode

RSVP interface configuration

1.38.3 Syntax Description

key-chain	Name of the key chain used for authentication.

1.38.4 Default

Authentication is not enabled.

1.38.5 Usage Guidelines

Use the **authentication** command to enable authentication for an RSVP interface.

Key chains allow you to control authentication for SmartEdge router routing protocols. Neighboring routers using RSVP to exchange reservation and path messages must utilize an accepted key ID and key string. If multiple key IDs have been configured, the one with the most recent send time exceeded the current time is used. All key IDs that have not expired and that have a receive time exceeding the current time are accepted.

Routes within the same area are not required to use the same authentication key ID. However, if two routers directly exchange updates, they must have the same authentication key ID.

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

1.38.6 Examples

The following example shows how to configure authentication for the RSVP interface, `192.169.1.2`:

```
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#interface 192.169.1.2
[local]Redback(config-rsvp-if)#authentication auth01
```

1.39 authentication (VRRP)

authentication {**none** | **redback-md5** ***key-chain-name*** | **simple** ***key-chain-name***}

{**no** | **default**} **authentication**

1.39.1 Purpose

Configures authentication of Virtual Router Redundancy Protocol (VRRP) exchanges.

1.39.2 Command Mode

VRRP configuration

1.39.3 Syntax Description

none	Specifies no authentication.
redback-md5 ***key-chain-name***	Redback Message Digest 5 (MD5) authentication key chain name.
simple ***key-chain-name***	Simple authentication key chain name.

1.39.4 Default

Authentication is not enabled.

1.39.5 Usage Guidelines

Use the **authentication** command to enable authentication of VRRP exchanges.

Use the **no** or **default** form of this command to disable authentication of VRRP exchanges.

1.39.6 Examples

The following example shows how to configure a virtual router owner using our proprietary MD5 authentication:

```
[local]Redback(config-ctx)#interface one
[local]Redback(config-if)#ip address 10.1.1.1/24
[local]Redback(config-if)#vrrp 1 owner
[local]Redback(config-vrrp)#authentication redback-md5 redback-md5-chain
[local]Redback(config-vrrp)#exit
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#key-chain redback-md5-chain key-id 1 key-string secret
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port ethernet 7/2
[local]Redback(config-port)#bind interface one local
[local]Redback(config-port)#no shutdown
```

1.40 auto-cost

auto-cost [**reference-bandwidth** *bandwidth*]

no auto-cost

default fault auto-cost

1.40.1 Purpose

Specifies that the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) interface cost is computed automatically, and configures the reference bandwidth that is used in the interface cost computation.

1.40.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.40.3 Syntax Description

reference-bandwidth *bandwidth*	Optional. Bandwidth rate in Mbps. The range of values is 1 to 4,294,967; the default value is 100.

1.40.4 Default

The interface cost is computed automatically using a reference bandwidth of 100 Mbps.

1.40.5 Usage Guidelines

Use the **auto-cost** command to specify that the OSPF or OSPFv3 interface cost is computed automatically and to configure the reference bandwidth that is used in the interface cost computation. The interface cost is computed by dividing the reference bandwidth by the interface speed. A cost of one is assigned if the interface speed is greater than the reference bandwidth.

You can override the automatic cost setting on individual interfaces by issuing the **cost** command in OSPF or OSPF3 interface configuration mode.

Use the **no** form of this command to disable automatic cost computation.

Use the **default** form of this command to return the reference bandwidth to 100 Mbps.

1.40.6 Examples

The following example shows how to configure the OSPF bandwidth rate to 64 Mbps:

```
[local]Redback(config-ospf)#auto-cost reference-bandwidth 64
```

1.41 auto-edge

auto-edge

no auto-edget

1.41.1 Purpose

Enables automatic detection of a Rapid Spanning Tree Protocol (RSTP) edge port.

1.41.2 Command Mode

Spanning-tree profile configuration

1.41.3 Syntax Description

This command has no keywords or arguments.

1.41.4 Default

The associated port is not enabled to automatically detect whether it is an RSTP edge port.

1.41.5 Usage Guidelines

Use the **auto-edge** command to enable ports to automatically detect whether it is an RSTP edge port.

The **auto-edge** option is one of several options in the RSTP profile which can be assigned to ports as is shown in the following example:

1.41.6 Examples

The following example illustrates how the **spanning-tree profile** command creates the spanning-tree profile womp and configures it for automatic edge port detection. In the second part of the example, an Ethernet port is assigned the spanning-tree profile womp and, therefore, is configured as an RSTP port with automatic edge port detection:

```
[local]Redback(config)#spanning-tree profile womp
[local]Redback(config-stp-prof)#auto-edge
[local]Redback(config-stp-prof)#exit
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#spanning-tree profile womp
```

1.42 auto-negotiate

auto-negotiate [**flc** *flow-control*] [**force** *port-state*] [**speed** *speed*] [**duplex** *mode*]

no auto-negotiate

default auto-negotiate [**flc** | **force**]

1.42.1 Purpose

Configures the auto-negotiation parameters for this Gigabit Ethernet (GE) port; if this port is a SmartEdge 100 GE port with a copper interface, specifies the values for the port speed and duplex mode to be negotiated. This command does not apply to ports on the 10 Gbps GE (10GE) or Fast Ethernet (FE) line cards.

1.42.2 Command Mode

Port configuration

1.42.3 Syntax Description

flc *flow-control*

Optional. Configures the negotiated parameter set for flow control, according to one of the following keywords:

- **off**—Sets flow control to off.
- **tx-only**—Negotiates the use of flow control in the send (Tx) direction only.
- **tx&rx**—Negotiates the use of flow control in both the send (Tx) and receive (Rx) directions.
- **tx&rx-or-rx-only**—Negotiates the use of flow control either in both the send (Tx) and receive (Rx) directions or in only the receive direction. This is the default setting.

force *port-state*

Optional. Specifies the port state settings to be applied if auto-negotiation fails, according to one of the following keywords:

- **enable**—Sets the port state to up if auto-negotiation fails, and sets the flow control using the value specified by the **flow-control** command (in port configuration mode).
- **disable**—Sets the port state to down if auto-negotiation fails, and continues to negotiate indefinitely. This is the default setting.

speed ***speed*** Optional. If this is a SmartEdge 100 GE port with a copper interface, specifies the port speed to be negotiated according to one of the following keywords:

- **1000**—Specifies the port speed to be negotiated as 1 Gbps; this is the default setting.
- **100**—Specifies the port speed to be negotiated as 100 Mbps.
- **10**—Specifies the port speed to be negotiated as 10 Mbps.
- **10-or-100**—Specifies the port speed to be negotiated as 10 or 100 Mbps, subject to auto-negotiation.

duplex ***mode*** Optional. If this is a SmartEdge 100 GE port with a copper interface, specifies the duplex mode to be negotiated, according to one of the following keywords:

- **full**—Specifies the port duplex mode to be negotiated as full duplex; this is the default setting.
- **half**—Specifies the port duplex mode to be negotiated as half-duplex.
- **full-or-half**—Specifies the port duplex mode to be negotiated as half- or full- duplex.

1.42.4 Default

Auto-negotiation is enabled on GE ports. The SmartEdge router negotiates flow control in either both send (Tx) and receive (Rx) directions or in the receive direction only. Force mode is disabled. The port speed and duplex mode to be negotiated for any SmartEdge 100 GE port with a copper interface is 1 Gbps in full duplex mode.

1.42.5 Usage Guidelines

Use the **auto-negotiate** command to configure the auto-negotiation parameters for this GE port; for a SmartEdge 100 GE port with a copper interface, this command specifies the values for the port speed and duplex mode to be negotiated.

When auto-negotiation is enabled, the values specified in the flc construct specify the flow control parameters:

- When auto-negotiation is enabled and force mode is disabled, the port remains down if negotiation fails.
- When auto-negotiation is enabled and force mode is enabled, the port comes up if the negotiation fails and the flow control mode is set using the

value configured by the **flow-control** command (in port configuration mode).

A SmartEdge 100 GE port supports multiple speeds when configured using one of the following copper-based interfaces:

- Native port RJ-45 connector on the chassis front panel
- Copper GE media interface card (MIC)

Use the **speed** *speed* and **duplex** *mode* constructs to specify the speed and duplex mode to be negotiated for one of these ports. If auto-negotiation fails when the value specified for the port speed is 10 or 100, the speed is set to auto-sense and the duplex mode to half-duplex. If auto-negotiation fails when the value specified for the port speed is 1000, the copper-based SmartEdge 100 GE port cannot come up.

Use the **no** form of the command to disable auto-negotiation. This form of the command effectively places the port into force mode. In this case, the port comes up if the negotiation fails, and the flow control mode is set using the value configured by the flow-control command (in port configuration mode).

Use the **default** form of this command to specify the default condition.

Note: Auto-negotiation and flow control may yield different results and behavior in configuration files created before Release 4.0.5 of the operating system software.

Note: IEEE 802.3 1000Base-T interfaces rely on auto-negotiation to determine which peer provides link timing. Auto-negotiation must be enabled on all SmartEdge 1000Base-T interfaces to ensure the correct behavior.

1.42.6 Examples

The following example shows how to enable auto-negotiation and force mode. If negotiation succeeds, the SmartEdge router negotiates flow control to transmit-only. If negotiation fails, the port comes up and flow control is set using the value configured by the flow-control command (in port configuration mode):

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#auto-negotiate flc tx-only force enable
```

The following example shows how to set auto-negotiation and negotiated flow control parameter values to the default, leaving the configured value for force mode still in effect:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#default auto-negotiate flc
```

1.43 auto-revert-delay

auto-revert-delay *seconds*

no auto-revert-delay *seconds*

1.43.1 Purpose

Enables auto-revert on a redundant pair of L2VPN XCs and sets the auto-revert timer for L2VPN XC redundancy.

1.43.2 Command Mode

L2VPN profile peer configuration

1.43.3 Syntax Description

seconds	Number of seconds that must pass before the operating system switches from the backup XC to the primary XC after the primary comes back up. Range is from 0 through 180 seconds.

1.43.4 Default

Auto-revert is disabled.

1.43.5 Usage Guidelines

Use the **auto-revert-delay** command to enable auto-revert on a redundant pair of L2VPN XCs and sets the auto-revert timer for L2VPN XC redundancy.

Use the **no** version of this command to disable auto-revert on a redundant pair of L2VPN XCs.

1.43.6 Examples

The following example shows how to set the auto-revert delay time on a redundant pair of L2VPN XCs to be 100 seconds:

```
[local]Redback(config)#l2vpn profile p1
[local]Redback(config-l2vpn-xc-profile)#peer 100.100.100.1
[local]Redback(config-l2vpn-xc-profile-peer)#auto-revert 100
```

1.44 backup-peer

backup-peer ***peer-address***

no backup-peer ***peer-address***

1.44.1 Purpose

Specifies the remote end of a backup L2VPN XC in a redundant pair of L2VPN XCs and enters L2VPN profile backup peer configuration mode.

1.44.2 Command Mode

L2VPN profile peer configuration

1.44.3 Syntax Description

peer-address	IP address of the remote end of a backup peer in a redundant pair of L2VPN XCs.

1.44.4 Default

No backup peer is specified.

1.44.5 Usage Guidelines

Use the **backup-peer** command to specify the remote end of a backup L2VPN XC in an L2VPN profile and enter L2VPN profile backup peer configuration mode.

For a redundant XC pair to use a backup L2VPN that is specified in an attached L2VPN profile, the backup peer in the XC configuration must match the backup peer that is specified in the L2VPN profile. Use the **xc** command in primary L2VPN XC configuration mode to specify a backup peer in an XC configuration, as shown in the following example:

```
[local]Redback(config-l2vpn-xc-group)#xc 10/3 vlan-id 100 vc-id 100 profile vlan6 backup
[local]Redback(config-l2vpn-xc-prime]#vc-id 200 peer 100.100.100.2
```

Use the *tunnel ldp-path* or *tunnel lsp* command in L2VPN profile backup peer configuration mode to configure the backup peer in the L2VPN profile configuration.

Note: Specifying a backup peer in an L2VPN profile is optional.

Use the **no** form of the **backup-peer** command to remove the specification of the remote end of a backup XC from an L2VPN profile.

1.44.6 Examples

The following example shows how to specify the remote end of a backup L2VPN XC in an L2VPN profile:

```
[local]Redback(config)#l2vpn profile vlan6
[local]Redback(config-l2vpn-xc-profile)#backup-peer 100.100.100.2
```

1.45 bandwidth

bandwidth ***value***

1.45.1 Purpose

Specifies the bandwidth reserved by an interface.

1.45.2 Command Mode

RSVP interface configuration

1.45.3 Syntax Description

value	Bandwidth value. If no unit is specified, the value is in bytes per second. The bandwidth value is signaled to the other Resource Reservation Protocol (RSVP) peers. In RSVP LSP configuration mode, the valid values are 1 to 1000000000. In RSVP interface configuration command mode, the valid values are 1 to 4294967295.

1.45.4 Default

In RSVP LSP configuration mode, no extra bandwidth is reserved. In RSVP interface configuration mode, the extra bandwidth on the interface is reserved.

1.45.5 Usage Guidelines

- Use the **bandwidth** command to specify the bandwidth reserved by an interface. This bandwidth value overrides the bandwidth reservation

calculated by setting the oversubscription factor. Otherwise, you can use the **over-subscription-factor** command (in RSVP router configuration mode) to reserve bandwidth, which is multiplied against available bandwidth and added to the subscribed amount.

Use the **no bandwidth** command to remove bandwidth to be reserved by an interface.

1.45.6 Examples

The following example shows how to specify the reserved bandwidth for the interface `if.1` to be 3 megabytes per second:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp-if)#interface if.1
[local]Redback(config-rsvp-lsp)#bandwidth 3 mbps
```

1.46 banner exec

banner exec ***delimited-text***

no banner exec

1.46.1 Purpose

Creates a message that displays after a user logs on to the system.

1.46.2 Command Mode

Global configuration

1.46.3 Syntax Description

delimited-text	Alphanumeric text to be displayed, using a delimiting character at the beginning and end of the message.

1.46.4 Default

No banner is defined.

1.46.5 Usage Guidelines

Use the **banner exec** command to create a message that displays after a user logs on to the system. The system accepts multiple lines of input; you must enter the matching delimiter to end the message. You can use any character as the delimiting character.

Use the **no** form of this command to delete the message. You do not need to delete an existing message to change it. When you create a new message, the old one is overwritten.

1.46.6 Examples

The following example shows how to configure a message to be displayed after users log on to the system. The message is delimited by the forward slash (/) character:

```
[local]Redback(config)#banner exec /Logged in to system Redback. Welcome to exec mode/
```

The following example shows how to configure a message using the letter z as the delimiting character:

```
[local]Redback(config)#banner exec zWarning - System going down at 0400.z
```

Users then see the following output after logging on to the system:

```
Redback login:administratorjeanne

password:xxxxxxxx


System going down at 0400.


[local]Redback#
```

1.47 banner login

banner login ***delimited-text***

no banner login

1.47.1 Purpose

Creates a message that displays after a user logs on to the system.

1.47.2 Command Mode

Global configuration

1.47.3 Syntax Description

delimited-text	Alphanumeric text to be displayed, using a delimiting character at the beginning and end of the message.

1.47.4 Default

No login banner is defined.

1.47.5 Usage Guidelines

Use the **banner login** command to create a message that displays after a user logs on to the system. The system accepts multiple lines of input; you must enter the matching delimiter to end the message. You can use any character as the delimiting character.

Note: The message displays only for Telnet and Secure Shell (SSH) sessions.

Use the **no** form of this command to delete the message. You do not need to delete an existing message to change it. When you create a new message, the old one is overwritten.

1.47.6 Examples

The following example shows how to configure a message to be displayed when a user logs on to the system, using the forward slash (/) character as the delimiter:

```
[local]Redback(config)#banner login /Welcome to ABC. Unauthorized access is prohibited./
```

Users then see the following output after logging on to the system:

```
Redback login:administratorlassie
password:xxxxxxxx

Welcome to ABC. Unauthorized access is prohibited.

[local]Redback#
```

1.48 banner motd

banner motd ***delimited-text***

no banner motd

1.48.1 Purpose

Creates a message of the day (MOTD) that displays before the logon prompt on all connected systems.

1.48.2 Command Mode

Global configuration

1.48.3 Syntax Description

delimited-text	Alphanumeric text to be displayed, using a delimiting character at the beginning and end of the message.

1.48.4 Default

No MOTD banner is defined.

1.48.5 Usage Guidelines

Use the **banner motd** command to create an MOTD to display before the logon prompt. The system accepts multiple lines of input; you must enter the matching delimiter to end the message. You can use any character as the delimiting character.

Note: The message displays only for Telnet and Secure Shell (SSH) sessions.

Use the **no** form of this command to delete the message. You do not need to delete an existing message to change it. When you create a new message, the old one is overwritten.

1.48.6 Examples

The following example shows how to configure a message to be displayed before the logon prompt on all connected systems:

```
[local]Redback(config)#banner motd /Welcome to system Redback./
```

Users then see the following output before logging on to the system:

```
Welcome to system Redback.


Redback login:
```

1.49 bert

For ports on channelized OC-12 line cards, the syntax is:

bert *slot/port*:*ds3-chan-num*[:*ds1-chan-num*] **pattern** *pattern* **interval** *minutes* [**error** *error*]

no bert *slot/port*:*ds3-chan-num*[:*ds1-chan-num*]

For channelized ports on DS-3 line cards, the syntax is:

bert *slot/port*[:*ds1-chan-num*] **pattern** *pattern* **interval** *minutes* [**error** *error*]

no bert *slot/port*[:*ds1-chan-num*]

For clear-channel ports on DS-3 or E3 line cards, the syntax is:

bert *slot/port* **pattern** *pattern* **interval** *minutes* [**error** *error*]

no bert *slot/port*

For ports on Asynchronous Transfer Mode (ATM) DS-3 line cards, the syntax is:

bert *slot/port* **pattern** *pattern* **interval** *minutes* [**error rate** *milliseconds*]

no bert *slot/port*

1.49.1 Purpose

Starts a bit error rate test (BERT) on an ATM DS-3, clear-channel DS-3, or E3 port, or a DS-1 or clear-channel DS-3 channel.

1.49.2 Command Mode

Exec

1.49.3 Syntax Description

slot	Chassis slot number for the card for which a BERT is started.
port	Port number for which a BERT is started.
ds3-chan-num	Channelized or clear-channel DS-3 channel number for which a BERT is started. The range of values is 1 to 12.
ds1-chan-num	Optional. DS-1 channel number for which a BERT is started. The range of values is 1 to 28.
pattern ***pattern***	Test data pattern, according to one of the types listed in Table 9.
interval ***minutes***	Test duration in minutes. The range of values is 1 to 1,440.
error ***error***	Optional. Number of injected bit errors, according to one of the keywords listed in Table 10. The default value is **none**.
error rate ***milliseconds***	Optional. Number of milliseconds between injected error bits; the value must be in multiples of 100 milliseconds. This construct is for ATM DS-3 ports only.

1.49.4 Default

No BERT is started.

1.49.5 Usage Guidelines

Use the **bert** command to start a BERT on a channel or port.

Note: The SmartEdge 100 router does not support this command.

Not all patterns are supported on all channels or ports. Table 9 lists the patterns and the channels and ports that support them.

Table 9 Supported BERT Patterns for Ports and Channels

Pattern Keyword	Description	Ports or Channels			
ATM DS-3	**DS-3**	**DS-1**	**E3**		
`0s`	Specifies all zeros as the test pattern.	No	Yes	Yes	Yes
`1-in-2`	Specifies a 1 in 2 (alternate 1s and 0s) test pattern.	No	No	No	Yes
`1-in-8`	Specifies a 1 in 8 test pattern.	No	Yes	Yes	Yes
`1-in-12`	Specifies a 1 in 12 test pattern.	No	Yes	Yes	No
`1-in-32`	Specifies a 1 in 32 test pattern.	No	Yes	Yes	No
`1s`	Specifies all ones as the test pattern.	Yes	Yes	Yes	Yes
`2^15`	Specifies a 2^15 test pattern.	Yes	Yes	Yes	Yes
`2^20`	Specifies a 2^20 test pattern.	No	Yes	Yes	Yes
`2^23`	Specifies a 2^23 test pattern.	Yes	Yes	Yes	Yes
`qrss`	Specifies 2^20-1 quasi random signal source (QRSS) O.151 test pattern.	No	Yes	See Note	No
`user-defined`	User-defined pattern with the pattern immediately following.	No	Yes	Yes	No
`1100`	Specifies a 1100 test pattern.	Yes	No	No	Yes

Note: The QRSS pattern is available for only for DS-1 channels on the 3-port channelized DS-3 line card.

Table 10 lists the number of bit errors that you can inject for DS-3 channels or ports.

Table 10 Number of Injected Bit Errors

Keyword	Description
`10^3`	Specifies a 1-bit error in 10^3 bits.
`10^4`	Specifies a 1-bit error in 10^4 bits.
`10^5`	Specifies a 1-bit error in 10^5 bits.
`10^6`	Specifies a 1-bit error in 10^6 bits.

Keyword	Description
10^7	Specifies a 1-bit error in 10^7 bits.
10^8	Specifies a 1-bit error in 10^8 bits.
10^9	Specifies a 1-bit error in 10^9 bits.
10^10	Specifies a 1-bit error in 10^10 bits.
none	Specifies no injected bit errors; this is the default value.

You can run a BERT on only one clear-channel DS-3 channel or port, E3 port, or all the DS-1 channels on a channelized DS-3 channel or port on a line card at any one time.

The keepalive function must be disabled on the DS-1 channel, DS-3 channel or port, or E3 port before you can run the BERT.

DS-1 channels do not support injected bit errors; if you include the **error** ***error*** construct when starting a BERT on a DS-1 channel, you must specify the **none** keyword.

ATM DS-3 ports do not support the **error** ***error*** construct. If you specify the **error rate** ***milliseconds*** construct for an ATM DS-3 port, you must specify the ***milliseconds*** argument in multiples of 100 milliseconds; an invalid value is rejected with an error message.

A user-defined test pattern consists of 8, 16, 24, or 32 bits in a 1- to 4-octet field. The bit transmission order is from least significant bit (LSB) to most significant bit (MSB). For example, the bit pattern 0x010203 is transmitted as the byte sequence 0xC04080.

Note: If you specify a 2^15 or 2^23 bit pattern for an E3 port and the far-end equipment is configured with the all-ones bit pattern, the E3 port synchronizes with the all-ones pattern and counts the deviations from the all-ones pattern instead of the configured pattern.

Similarly, if you specify a 2^20 bit pattern for an E3 port and the far-end equipment is configured with the all-zeros bit pattern, the E3 port synchronizes with the all-zeros pattern and counts the deviations from the all-zeros pattern instead of the configured pattern.

In either case, always verify that the configured bit patterns for the E3 port and far-end equipment match before running a BERT and interpreting the resulting status and statistics.

Note: When running BERT test patterns, an all-1s pattern causes the remote end to falsely detect an AIS alarm.

Use the **no** form of this command to stop the test.

1.49.6 Examples

The following example shows how to enable BERT on DS-3 port `1` on a channelized DS-3 line card, using a test pattern of all zeros, for `10` minutes with one injected bit error in `10^8` bits:

```
[local]Redback>bert 5/1 pattern 0s interval 10 error 10^8
```

The following example shows how to enable BERT on DS-3 port `1` on a channelized DS-3 line card, using a user-defined test pattern of `0x010203`, for `10` minutes with one injected bit error in `10^8` bits:

```
[local]Redback>bert 5/1 pattern user-defined 0x010203 interval 10 error 10^8
```

The following example shows how to enable BERT on port `3` on an ATM DS-3 line card, using a 2^15 bit pattern, for `3` minutes with an injected bit error every `100` milliseconds:

```
[local]Redback>bert 13/3 pattern 2^15 interval 3 error rate 100
```

1.50 bestpath med always-compare

bestpath med always-compare

no bestpath med always-compare

1.50.1 Purpose

Allows the comparison of the Multi-Exit Discriminator (MED) for paths from all Border Gateway Protocol (BGP) neighbors in different autonomous systems.

1.50.2 Command Mode

BGP router configuration

1.50.3 Syntax Description

This command has no keywords or arguments.

1.50.4 Default

By default, the MED comparison is performed by the BGP routing instance on BGP paths received from BGP neighbors in one other autonomous system. When enabled, this command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

1.50.5 Usage Guidelines

Use the **bestpath med always-compare** command to allow the comparison of the MED for paths from all BGP neighbors in different autonomous systems.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. By default, MED comparison is done only among paths from the same autonomous system. This command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

Use the **no** form of this command to disable the comparison of the MED for paths from BGP neighbors in different autonomous systems.

1.50.6 Examples

The following example shows how to enable the BGP speakers in autonomous system `64001` to compare the MED for paths from BGP neighbors in different autonomous systems:

```
[local]Redback(config)#router bgp 64001
[local]Redback(config-bgp)#bestpath med always-compare
```

1.51 bfd (BGP neighbor)

bfd

no bfd

1.51.1 Purpose

Enables Bidirectional Forwarding Detection (BFD) for an external Border Gateway Protocol (eBGP) neighbor.

1.51.2 Command Mode

BGP neighbor configuration

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

BFD is disabled.

1.51.5 Usage Guidelines

Use the **bfd** command to enable BFD for an eBGP neighbor.

BFD is a simple Hello protocol that provides the ability to detect communication failures in less than one second. When BFD detects a communication failure to the eBGP neighbor, the neighbor is reset.

Note: BFD can be enabled only for eBGP neighbors; enabling BFD for an internal BGP (iBGP) neighbor generates an error message.

Use the **no** form of this command to disable BFD for an eBGP neighbor.

1.51.6 Examples

The following example shows how to enable BFD for an eBGP neighbor with the IP address `192.168.1.1`:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bgp 64001
[local]Redback(config-bgp)#neighbor 192.168.1.1 external
[local]Redback(config-bgp-neighbor)#bfd
```

1.52 bfd (RSVP client)

bfd

no bfd

1.52.1 Purpose

Enables Bidirectional Forwarding Detection (BFD) on a Resource Reservation Protocol (RSVP) client.

1.52.2 Command Mode

RSVP router configuration

1.52.3 Syntax Description

This command has no keywords or arguments.

1.52.4 Default

BFD is disabled.

1.52.5 Usage Guidelines

Use the **bfd** command to enable BFD for an RSVP client.

When enabled on an RSVP client, BFD triggers fast reroute (FRR) when a down notification is received from a primary RSVP label-switched path (LSP). If a backup LSP is configured, that LSP becomes active. If the backup LSP is down and a backup-to-backup LSP is configured, the backup-to-backup LSP becomes active. When the down RSVP LSP comes back up, BFD triggers the RSVP primary LSP and attempts to reestablish the RSVP adjacency with the neighbor.

Note: For BFD to work, you must first enable BFD on the RSVP level, and then use the **interface** command in BFD router configuration mode to enable BFD for a specific next-hop neighbor.

Use the **no** form of this command to disable BFD for an RSVP client.

1.52.6 Examples

The following example shows how to enable BFD for an RSVP client:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#bfd
```

1.53 bfd-monitoring neighbor

bfd-monitoring neighbor *ip-addr*

no bfd-monitoring neighbor *ip-addr*

1.53.1 Purpose

Enables BFD liveliness detection on the specified neighbor.

1.53.2 Command Mode

VRRP configuration mode.

1.53.3 Syntax Description

ip-addr	IP address of the BFD neighbor you want to track.

1.53.4 Default

BFD liveliness detection is disabled on a neighbor.

1.53.5 Usage Guidelines

Use the **bfd-monitoring neighbor** command to enable BFD liveliness detection for the specified neighbor.

During switchover, traffic may be lost for up to three VRRP advertisement intervals because the standby XCRP does not support VRRP in hot standby mode. If the VRRP advertisement interval has been configured in milliseconds (with the **advertise interval** command), the interval reverts to the default value, where VRRP advertisements are sent out every second.

Note: For BFD liveliness detection to work, BFD must be enabled on the VRRP interface that connects the master and backup VRRP routers. BFD liveliness detection is supported on backup VRRP routers only.

Use the **no** form of this command to disable BFD liveliness detection for a neighbor.

1.53.6 Examples

The following example shows how to configure the backup VRRP router `1` to track the neighbor with the IP address of `129.100.0.1`:

```
[local]SE1(config)#context local
[local]SE1(config-ctx)#interface vlan1
[local]SE1(config-if)#vrrp 1 backup
[local]SE1(config-vrrp)#bfd-monitoring neighbor 129.100.0.1
```

1.54 bind authentication

bind authentication {**pap** | **pap chap** | **chap** | **chap pap**} [**maximum** *max-sess*] [**context** *ctx-name* | **service-policy** *svc-policy-name*]

no bind

1.54.1 Purpose

Creates a dynamic binding between an access link group, a Fast Ethernet (FE) or Gigabit Ethernet (GE) port, an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), an 802.1Q PVC, or a child circuit on an ATM or 802.1Q PVC, which is configured with Point-to-Point Protocol (PPP) or PPP over Ethernet (PPPoE) encapsulation, and an interface, using the specified PPP authentication protocol.

1.54.2 Command Mode

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

1.54.3 Syntax Description

pap	Specifies that the PPP authentication protocol to be used is Password Authentication Protocol (PAP).
pap chap	Specifies that either PAP or Challenge Handshake Authentication Protocol (CHAP) can be used, with PAP negotiated first.

chap	Specifies that the PPP authentication protocol to be used is CHAP.
chap pap	Specifies that either CHAP or PAP can be used, with CHAP negotiated first.
maximum *max-sess*	Optional. Maximum number of concurrent sessions allowed on a circuit or port. The range of values is 2 to 32,000 for an access link group or 1 to 32,000 for a port, PVC, or child circuit. This construct applies only to access link groups, circuits, and ports with PPPoE encapsulation.
context *ctx-name*	Optional. Name of the context to which PPP or PPPoE sessions on the circuit or port being bound are restricted.
service-policy *svc-policy-name*	Optional. Name of the service access control list (ACL) that defines the services available to the PPP-encapsulated circuit or port.

1.54.4 Default

None

1.54.5 Usage Guidelines

Use the **bind authentication** command to create a dynamic binding between an access link group, an FE or a GE port, an ATM PVC, an 802.1Q PVC, or a child circuit on an ATM or 802.1Q PVC, which is configured with PPP or PPPoE encapsulation, and an interface, using the specified PPP authentication protocol. This command is available only for a port, ATM PVC, 802.1Q PVC, or child circuit that has been previously configured with PPPoE or one of the PPP encapsulation types.

The ATM or 802.1Q PVC can be a static or on-demand circuit.

Note: You do not bind dynamic clientless IP service selection (CLIPS) PVCs; they are effectively bound by the **service clips** command (in port configuration mode).

The string configured with the **password** command (in port configuration mode) must match the password string sent by the remote PPP subscriber to the SmartEdge router.

Use the **chap** keyword to provide authentication without sending clear text passwords over the network. In the case of CHAP, the passwords referred to are actually shared secret keys used by the various systems to compute and verify cryptographic checksums in response to their peer's challenge. To the command-line interface (CLI), however, these values are run identically to the way PAP passwords are typed. The **password** command is used in all cases.

The **pap chap** construct specifies that PAP is negotiated first, with CHAP as a secondary choice. This configuration contradicts RFC 1334, PPP Authentication Protocols, but can potentially cause reduced security because CHAP-only clients use an encrypted exchange for authorization, but passwords are sent unencrypted with PAP. If a client is configured to accept both PAP and CHAP, only PAP is negotiated because with this bind configuration, PAP is offered first.

You cannot bring up a PPP link until the subscriber name and password negotiations have been completed and authorization has been granted.

If you are using the CHAP, PAP, or both authentication protocols, the response from the RADIUS server (in attribute 18) is forwarded to the PPP client with the reason for the acceptance or rejection of the subscriber.

The optional **maximum** ***max-sess*** construct is relevant only to access link groups, circuits, and ports with PPPoE encapsulation.

If you specify restricted dynamic binding (with the **context** ***ctx-name*** construct), the subscriber is authenticated based on the authentication, authorization, and accounting (AAA) configuration defined within that context. For information about configuring AAA features, see *Configuring Authentication, Authorization, and Accounting*.

If authentication is being done remotely using Remote Authentication Dial-In User Service (RADIUS), the local subscriber record is replaced by the corresponding subscriber record in the RADIUS database. For further information about RADIUS, see *Configuring RADIUS*.

When using global authentication, the Context-Name attribute returned by RADIUS must be identical to a context-name or a domain alias configured in the SmartEdge OS; otherwise the binding fails.

If you specify the optional **service-policy** ***svc-policy-name*** construct, all attempts to authenticate to contexts or domains not permitted by the named service policy fail.

If you modify a subscriber record for a subscriber that is already bound, you must use the **clear subscriber** command (in exec mode) for the changes to take effect. The subscriber session is ended and restarted with the new parameters. This is true regardless of whether subscriber records are configured locally or in RADIUS.

The IP address configured for a subscriber, either in a local subscriber record or that obtained from a RADIUS server, must fall within the range (address and network mask) of an interface that is defined within the context and to which that subscriber is to be bound. Otherwise, the bind fails and the PPP-encapsulated circuit does not come up.

If you enter a new bind authentication command for a child circuit created on an ATM PVC, the existing binding is not removed and no error message displays. To replace the existing binding, you must enter the no form of this command,

and then enter the bind authentication command with the new keywords and arguments.

If you enter a new **bind authentication** command for a port, channel, ATM PVC, or 802.1Q PVC, the existing binding is removed and any active sessions are dropped. If an existing binding is exactly the same as that specified in the new **bind authentication** command, the existing binding is not removed.

Note: The SmartEdge router uses the system hostname as the subscriber name string for all outbound PPP authentication.

Use the **no** form of this command to remove the binding.

1.54.6 Examples

The following example shows how to set the encapsulation to PPP on an ATM PVC on an ATM OC port, and then bind the PVC using CHAP or PAP, with CHAP offered first:

```
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#atm pvc 100 4 profile oam encapsulation ppp
[local]Redback(config-atm-pvc)#bind authentication chap pap
```

1.55 bind auto-subscriber

In ATM PVC or dot1q PVC configuration mode, the command syntax is:

bind auto-subscriber *prefix1 ctx-name* [**password** *prefix2*]

no bind

In CLIPS PVC configuration mode, the command syntax is:

bind auto-subscriber *prefix1 ctx-name* [**password** *password*]

no bind

1.55.1 Purpose

Automatically generates a **bind subscriber** command with a unique subscriber name for each Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) in a range of static or on-demand PVCs, for each 802.1Q PVC in a range of on-demand PVCs, or for each clientless IP service selection (CLIPS) static circuit in a range of CLIPS static circuits.

1.55.2 Command Mode

- ATM PVC configuration

- CLIPS PVC configuration
- dot1q PVC configuration
- Link PVC configuration

1.55.3 Syntax Description

prefix1	Leading text string for each subscriber name.
ctx-name	Name of the context to locate the subscriber information.
password ***prefix2***	Optional. Leading text string for each subscriber password on an ATM PVC.
password ***password***	Optional. Password for each subscriber on a CLIPS PVC.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **bind auto-subscriber** command to automatically generate **bind subscriber** commands with unique subscriber names and optional passwords for each static or on-demand ATM PVC, on-demand 802.1Q PVC, or CLIPS static circuit in the range.

For ATM PVCs, you use this command with the **atm pvc explicit** or **atm pvc on-demand** form of the **atm pvc** command in ATM OC configuration mode to create a range of PVCs.

This command is not available if the ATM PVCs are encapsulated using the **raw** or **pppoe** keywords. The generated subscriber names and passwords are of the following forms:

- Subscriber name: ***prefix1vpi.vci@ctx-name***
- Password: ***prefix2vpi.vci***

Note: The virtual path identifier (VPI) and virtual circuit identifier (VCI) are not assigned to an on-demand ATM PVC until the PVC is made active.

For 802.1Q PVCs, you use this command with the **dot1q pvc on-demand** form of the **dot1q pvc** command in port configuration mode or link PVC configuration mode; it is not available for a range of static 802.1Q PVCs.

The generated subscriber names and passwords are of the following formats:

- Subscriber name: ***prefix1vlan-id@ctx-name***
- Password: ***prefix2vlan-id***

  Note: The virtual LAN (VLAN) tag value is not assigned to an on-demand 802.1Q PVC until the PVC is made active.

  Note: The **@** separator character in the ATM and 802.1Q formats is not configurable.

For CLIPS static circuits, you use this command with the **clips pvc** command in port, dot1q PVC, or ATM PVC configuration mode.

The generated subscriber names are of the following forms for the CLIPS static circuits:

- Subscriber name: ***prefix1sess-num@ctx-name***
- Password: ***password***

In this case, the same password is assigned to each subscriber.

The character that separates the ***ctx-name*** argument from the circuit identifier is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see *Configuring Authentication, Authorization, and Accounting*. The default is @, which is used throughout this document.

The IP address configured for a subscriber, either in a local subscriber record or that obtained from a Remote Authentication Dial-In User Service (RADIUS) server, must fall within the range (address and network mask) of an interface that is defined within the context and to which that subscriber is to be bound. Otherwise, the bind fails and the PPP-encapsulated circuit does not come up.

If you enter a new **bind** command for an ATM or CLIPS static PVC, the previous binding is removed and any active sessions are dropped. If an existing binding on the ATM or CLIPS static PVC is exactly the same as that specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the automatically generated subscriber bindings.

1.55.6 Examples

The following example shows how to create 10 ATM PVCs with a virtual path identifier (VPI) value of `100`, and virtual channel identifier (VCI) values ranging from `100` to `109`, then use the **bind auto-subscriber** command to bind each PVC to an automatically generated subscriber name beginning with the string `DSL:`

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-port)#atm pvc explicit 100:100 through 109 profile encapsulation route1483
[local]Redback(config-pvc)#bind auto-subscriber DSL local
```

The following example shows how to create 10 CLIPS static circuits with session numbers ranging from `1` to `10` on Ethernet port `1`, then use the **`bind auto-subscriber`** command to bind each CLIPS static circuit to an automatically generated subscriber name beginning with the string `10-1-1-:`

```
[local]Redback(config)#port ether 4/1
[local]Redback(config)#service clips
[local]Redback(config-port)#clips pvc 1 through 10
[local]Redback(config-clips-pvc)#bind auto-subscriber "10-1-1-" local
```

1.56 bind bypass

`bind bypass`

`no bind bypass`

1.56.1 Purpose

Binds a circuit that is to be cross-connected.

1.56.2 Command Mode

- ATM child circuit configuration
- ATM PVC configuration
- dot1q child circuit configuration
- dot1q PVC configuration

1.56.3 Syntax Description

This command has no keywords or arguments.

1.56.4 Default

None

1.56.5 Usage Guidelines

Use the **bind bypass** command to bind a circuit that is to be cross-connected. Circuits include Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs), ATM child circuits, 802.1Q PVCs, Q-in-Q PVCs, and 802.1Q child circuits.

Note: If you do not enter this command when configuring the PVC or child circuit, the configuration is incomplete and the status of the cross-connection is not displayed in the output of the **show bypass** command (in any mode).

Use the **no** form of this command to remove the binding.

1.56.6 Examples

The following example shows how to bind an 802.1Q PVC with the VLAN tag value 100 on Ethernet port 1/1 before the PVC is cross-connected:

```
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 100 encapsulation raw
[local]Redback(config-dot1q-pvc)#bind bypass
```

1.57 bind interface

bind interface *if-name* {*ctx-name* | **local**}

no bind *if-name* {*ctx-name* | **local**}

1.57.1 Purpose

Statically binds a port, channel, permanent virtual circuit (PVC), an 802.1Q tunnel, a link group, a Generic Routing Encapsulation (GRE) tunnel or tunnel circuit, an IP-in-IP tunnel, or an overlay tunnel to a previously created interface in the specified context.

1.57.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Frame Relay PVC configuration
- Link group configuration

- Link PVC configuration
- Port configuration
- Tunnel configuration

1.57.3 Syntax Description

if-name	Name of a previously created interface.
ctx-name	Context name or a domain alias, which may be used in place of the context name.
local	The default context for the SmartEdge router as a whole is named, **local**.

1.57.4 Default

No ports, channels, PVCs, link groups, GRE tunnel circuits, or overlay tunnel circuits are bound.

1.57.5 Usage Guidelines

Use the **bind interface** command to statically bind a port, channel, PVC, 802.1Q tunnel, link group, GRE tunnel circuit, or overlay tunnel circuit to a previously created interface in the specified context. No data can flow through a port, a channel, a PVC, an 802.1Q tunnel, a child circuit, a link group, a tunnel, or a tunnel circuit until it is bound to an interface.

Note: The SmartEdge 100 router does not support ATM, on-demand ATM, Frame Relay, or 802.1Q PVCs.

Both the interface and specified context or domain alias, defined by the domain command (in context configuration mode), must exist before you enter the **bind interface** command. If either is missing, the system displays an error message.

To bind multiple circuits to a single interface, the specified interface must have been created using the **interface** command with the **multibind** keyword specified.

To display the state of the bindings for the interfaces in a context, enter the **show ip interface** command in any mode.

Use the **no** form of this command to remove the binding. You must remove any existing binding before you can create a new binding for the port, channel, PVC, link group or GRE tunnel circuit.

1.57.6 Examples

The following example shows how to bind a POS port to the interface, `SoHo1`, in the `local` context:

```
[local]Redback(config)#port pos 3/1
[local]Redback(config-port)#bind interface SoHo1 local
```

1.58 bind sse group

bind sse group ***group_name*** **[secondary]**

no bind sse group

1.58.1 Command Mode

Card configuration

1.58.2 Syntax Description

group_name	Name of the SSE group associated with this SSE card.
secondary	Configure the SSE card to be secondary in an SSE group. Applies only to network-redundant SSE groups.

1.58.3 Default

The SSE card is not assigned to an SSE group.

1.58.4 Usage Guidelines

Assigns an SSE card to an SSE group. Each SSE card can only be assigned to one group. Each SSE group can have a maximum of two SSE cards assigned.

To configure a network-redundant SSE card, create an SSE group with network redundancy configured and assign on SSE card as primary and another as secondary. Use the ***secondary*** keyword to assign an SSE card as secondary in a network-redundant SSE group; issue the **bind sse group** command without the ***secondary*** keyword to assign the SSE card as primary.

To configure a disk-redundant SSE card, create an SSE group with disk redundancy configured and assign the SSE card to the group.

If you issue the **no** form of the command on the active card during data synchronization on any of the partitions, the following warning message appears:

```
Note: Executing the command during data
synchronization on any of the partitions will cause
data corruption.

Commit to continue; abort to exit without change.
```

Before you decommission an SSE card, you must remove it from any SSE group to which it is assigned, using the **no bind sse group** ***name*** command.

Caution!

Risk of data corruption and loss of charging records. Removing an SSE card from configuration without first shutting it down can cause file corruption. To avoid the risk, first enter the **no bind sse group** ***name*** and **commit** commands. Wait at least 15 seconds for the card to completely shut down before entering the **no card sse** ***slot*** command. If the SSE card is not configured for redundancy, enter the **card sse** ***slot*** and **shutdown** commands and wait for 15 seconds before entering the **no card sse** ***slot*** command.

1.58.5 Examples

The following example shows how to configure an SSE card and assign it to an SSE group:

```
[local]Redback(config)#card sse 2
[local]Redback(config-card)#bind sse group sse_group_1
```

1.59 bind subscriber

bind subscriber ***sub-name@ctx-name*** [**password** ***password***]

no bind subscriber ***sub-name@ctx-name*** [**password** ***password***]

1.59.1 Purpose

Statically binds a single static or on-demand Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), a single static or on-demand 802.1Q PVC, or a single clientless IP service selection (CLIPS) static circuit indirectly to an interface by using the IP address within the local or Remote Authentication Dial-In User Service (RADIUS) subscriber record for the specified subscriber.

1.59.2 Command Mode

- ATM child circuit configuration
- ATM PVC configuration
- CLIPS PVC configuration
- dot1q child circuit configuration
- dot1q PVC configuration
- Link group configuration

1.59.3 Syntax Description

sub-name@ctx-name	Subscriber name and context name that define the subscriber record to be used. The combination of subscriber name and context name can be up to 253 characters, including the separator character.
password ***password***	Optional. Password string to be associated with the subscriber name. Required if the associated subscriber record or RADIUS record requires a password.

1.59.4 Default

None

1.59.5 Usage Guidelines

Use the **bind subscriber** command to statically bind a single static or on-demand ATM PVC, a single static or on-demand 802.1Q PVC, or a single CLIPS static circuit indirectly to an interface by using the IP address within the local or RADIUS subscriber record for the specified subscriber.

This command is not available for a single on-demand ATM PVC unless you have configured the PVC with the **aaa** keyword to use RADIUS to supply the binding.

You can specify a domain alias, defined by the domain command (in context configuration mode), in place of the context name. The subscriber password string, if supplied, is not encrypted in the configuration file. A password with embedded spaces can be entered by enclosing the entire password in double quotes; for example, "`This is a password`."

You can configure a custom structured format for the ***sub-name@ctx-name*** construct; see *Configuring Authentication, Authorization, and Accounting*.

Note: If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

1.59.6 Examples

The following example shows how to set the encapsulation on an ATM PVC to PPP on an ATM OC port, and then bind the PVC using the subscriber record, `george`, in the `local` context:

```
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#atm pvc 100 110 profile ubr1 encapsulation ppp
[local]Redback(config-atm-pvc)#bind subscriber george@local
```

The following example shows how to create a single static circuit on an Ethernet port and then bind the circuit using the subscriber record, `greg`, in the `local` context:

```
[local]Redback(config)#port ether 5/1
[local]Redback(config-port)#service clips
[local]Redback(config-port)#clips pvc 100
[local]Redback(config-clips-pvc)#bind subscriber greg@local
```

The following example shows how to set the encapsulation on an ATM PVC to PPPoE on an ATM OC port and then bind the PVC using the subscriber record, `george`, in the `local` context:

```
[local]Redback(config)#port atm 2/1
[local]Redback(config-port)#atm pvc 1 10 profile ubr encapsulation pppoe
[local]Redback(config-clips-pvc)#bind subscriber greg@local
```

1.60 block-flooding

block-flooding

no block-flooding

1.60.1 Purpose

Blocks the flooding of link-state advertisements (LSAs) that are not self-originated.

1.60.2 Command Mode

- OSPF interface configuration
- OSPF3 interface configuration

1.60.3 Syntax Description

This command has no keywords or arguments.

1.60.4 Default

Flooding of LSAs that are not self-originated is not blocked.

1.60.5 Usage Guidelines

Use the **block-flooding** command in highly meshed topologies to block the flooding of LSAs that are not self-originated.

Caution!

Risk of Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) routing errors. Blocking flooding on an interface can result in inconsistencies between OSPF or OSPFv3 routers and their respective route tables. To reduce the risk, exercise caution before blocking the flooding of LSAs that are not self-originated.

Use the **no** form of this command to remove the LSA flooding block.

1.60.6 Examples

The following example shows how to block flooding on the OSPF interface, `to-sj`:

```
[local]Redback(config-ospf)#area 0
[local]Redback(config-ospf-area)#interface to-sj
[local]Redback(config-ospf-if)#block-flooding
```

1.61 block-time

block-time ***block-secs***

no block-time

1.61.1 Purpose

Sets the initial time a circuit remains blocked after a bridging loop is detected.

1.61.2 Command Mode

Loop-detection configuration

1.61.3 Syntax Description

block-secs	Number of seconds to which the initial blocking time is set. The range of values is 0 to 3600.

1.61.4 Default

The initial block time is 60 seconds.

1.61.5 Usage Guidelines

Use the **block-time** command to set the initial time a circuit remains blocked after a bridging loop is detected.

The block time automatically doubles if bridging loops are detected in the same location in consecutive intervals.

When the block time passes, the circuit is unblocked. You can manually unblock circuits by using the **clear bridge loop-detect** command.

Use the **no** form of the command to return the block time to the default.

1.61.6 Examples

The following example illustrates setting the block time to `20` seconds:

```
[local]Redback(config)#context ink
[local]Redback(config-ctx)#bridge lbdl
[local]Redback(config-bridge)#loop-detection
[local]Redback(config-ld)#block-time 20
```

1.62 boot configuration

boot configuration *url*

no boot configuration *url*

default boot configuration

1.62.1 Purpose

Specifies a configuration file to be read when the system boots.

1.62.2 Command Mode

Global configuration

1.62.3 Syntax Description

url	URL of a configuration file to be read at boot time.

1.62.4 Default

The boot configuration file is `/flash/redback.cfg`.

1.62.5 Usage Guidelines

Use the **boot configuration** command to specify a configuration file to be read when the system is loaded after a power on sequence or a reload. When you enter this command, any previously configured boot configuration file is replaced.

You must specify a file on the local file system, with a URL in the following form:

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

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

Use the **no** form of this command to undo a previous **boot configuration** command. You must provide the same ***url*** argument provided in that previous command.

Use the **default** form of this command to set the configuration file to the default boot configuration file.

Note: The system loads the binary version of the redback.cfg file if it is available. The system creates the binary version when you enter the **save configuration** command (in exec mode) without specifying a filename.

1.62.6 Examples

The following example shows how to specify that the file, `old_config.cfg`, be loaded when the system is reloaded or powered on:

```
[local]Redback(config)#boot configuration /flash/old_config.cfg
```

The following example shows how to specify that the default configuration file be loaded when the system is reloaded or powered on:

```
[local]Redback(config)#default boot configuration
```

1.63 bootp-enable-auto

bootp-enable-auto

no bootp-enable-auto

1.63.1 Purpose

Enables the assignment of IP addresses from subnet ranges.

1.63.2 Command Mode

DHCP server configuration

1.63.3 Syntax Description

This command has no keywords or arguments.

1.63.4 Default

The assignment of IP addresses from subnet ranges is not enabled.

1.63.5 Usage Guidelines

Use the **bootp-enable-auto** command to enable the assignment of IP addresses from subnet ranges.

Note: The Bootstrap Protocol (BOOTP) allows certain systems to automatically discover network configuration information and boot information. The Dynamic Host Configuration Protocol (DHCP) is an extension of BOOTP that defines a protocol for passing configuration information to hosts on a Transmission Control Protocol (TCP)/IP network. For more information about BOOTP and DHCP, see RFC 2131, *Dynamic Host Configuration Protocol*.

If you do not enter this command, then you must enter the mac-address command (in DHCP subnet configuration mode); it is required for the DHCP server to assign IP addresses for BOOTP clients. If you enter this command, then you need not enter the mac-address command.

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

1.63.6 Examples

The following example shows how to specify the boot loader image file for the SmartEdge router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#bootp-enable-auto
```

1.64 bootp-filename

bootp-filename ***bootfile-name***

no bootp-filename ***bootfile-name***

1.64.1 Purpose

Specifies the filename of the boot loader image file.

1.64.2 Command Mode

DHCP server configuration

1.64.3 Syntax Description

bootfile-name Name of the boot loader image file.

1.64.4 Default

No boot loader image is specified.

1.64.5 Usage Guidelines

Use the **bootp-filename** command to specify the filename of the boot loader image file. The boot loader image file is run when the system is reloaded or powered on.

Note: The Bootstrap Protocol (BOOTP) allows certain systems to automatically discover network configuration information and boot information. The Dynamic Host Configuration Protocol (DHCP) is an extension of BOOTP that defines a protocol for passing configuration information to hosts on a Transmission Control Protocol (TCP)/IP network. For more information about BOOTP and DHCP, see RFC 2131, *Dynamic Host Configuration Protocol*.

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

1.64.6 Examples

The following example shows how to specify the boot loader image file for the SmartEdge router:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#bootp-filename of1267.bin
```

1.65 bootp-siaddr

bootp-siaddr ***ip-addr***

no bootp-siaddr ***ip-addr***

1.65.1 Purpose

Specifies the IP address that the boot loader client uses to download the boot loader image file.

1.65.2 Command Mode

DHCP server configuration

1.65.3 Syntax Description

ip-addr	IP address the boot loader client uses.

1.65.4 Default

No IP address is specified.

1.65.5 Usage Guidelines

Use the **bootp-siaddr** command to specify the IP address that the boot loader client uses to download the boot loader image file.

Note: The Bootstrap Protocol (BOOTP) allows certain systems to automatically discover network configuration information and boot information. The Dynamic Host Configuration Protocol (DHCP) is an extension of BOOTP that defines a protocol for passing configuration information to hosts on a Transmission Control Protocol (TCP)/IP network. The server's IP address (SIADDR) field in the DHCP packet specifies the address of the server to use in the next step of the client's bootstrap process. For more information about BOOTP, DHCP, and SIADDR see RFC 2131, *Dynamic Host Configuration Protocol*.

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

1.65.6 Examples

The following example shows how to specify the IP address for the SmartEdge router with the boot loader image file:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#bootp-siaddr 200.1.1.0
```

1.66 bpdu

bpdu {**deny** | **allow-only**}

no bpdu {**deny** | **allow-only**}

1.66.1 Purpose

Specifies whether the bridge drops or passes received Spanning Tree Bridge Protocol Data Units (BPDUs) and whether it drops or passes other received traffic.

1.66.2 Command Mode

Bridge profile configuration

1.66.3 Syntax Description

deny	Drop all received BPDUs and pass other received traffic.
allow-only	Pass all received BPDUs and drop all other received traffic.

1.66.4 Default

In the default condition, the bridge passes both received BPDUs and all other received traffic.

1.66.5 Usage Guidelines

The **bpdu** command specifies whether the bridge drops or passes received Spanning Tree BPDUs and whether it drops or passes other received traffic.

This feature applies to both IEEE BPDUs and Cisco proprietary PVST+ BPDUs.

You can apply BPDU filtering to the following:

- Bridged untagged Ethernet ports
- Bridged 802.1Q permanent virtual circuits (PVCs)
- Bridged 802.1Q PVCs within 802.1Q tunnels

The following restrictions apply:

- BPDU filtering does not operate on Virtual Private LAN Services (VPLS) pseudowire (PW) circuits

- Do not apply the **bpdu** command to circuits and ports of bridges enabled for Rapid Spanning Tree Protocol (RSTP).

Use the **no** form of this command to specify the default; namely, the bridge passes both received BPDUs and all other received traffic.

1.66.6 Examples

The following example shows how to configure the `prof-isp1 bridge profile to drop all received BPDUs:`

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(config-bridge-profile)#bpdu deny
```

1.67 bpdu priority

bpdu priority ***priority***

{**no** | **default**} **bpdu priority**

1.67.1 Purpose

Sets the priority of the incoming Spanning Tree Bridge Protocol Data Units (BPDUs).

1.67.2 Command Mode

Bridge profile configuration

1.67.3 Syntax Description

priority	Sets the priority of incoming BPDUs. The range of values for the ***priority*** argument is 0 to 7, where 0 is the highest priority and 7 is the lowest priority.

1.67.4 Default

In the default state, the priority of incoming BPDUs is not affected by this command.

1.67.5 Usage Guidelines

Use the **bpdu priority** command to specify the priority of incoming Spanning Tree BPDUs. The queuing of incoming packets is determined by their assigned priority.

This command overrides any QoS priority settings on the incoming BPDUs.

This feature applies to both IEEE BPDUs and Cisco proprietary PVST+ BPDUs.

You can apply BPDU queuing to the following:

- Bridged untagged Ethernet ports
- Bridged 802.1Q permanent virtual circuits (PVCs)
- Bridged 802.1Q PVCs within 802.1Q tunnels

The following restrictions apply:

- BPDU queuing does not operate on Virtual Private LAN Services (VPLS) pseudowire (PW) circuits.
- Do not apply the **bpdu priority** command to circuits and ports of bridges enabled for Rapid Spanning Tree Protocol (RSTP).

Use the **no** or **default** form of this command to return to the default state, in which the priority of incoming BPDUs is not affected by this command.

1.67.6 Examples

The following example shows how to configure `prof-isp1` bridge profile with a BPDU queue priority level of 3:

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(config-bridge-profile)#bpdu priority 3
```

1.68 bpdu rate-limit

bpdu rate-limit *rate* [**burst-size** *bpdus*]

{**no** | **default**} **bpdu rate-limit**

1.68.1 Purpose

Sets the maximum average rate and burst tolerance of received bridge protocol data units (BPDUs).

1.68.2 Command Mode

Spanning-tree configuration

1.68.3 Syntax Description

rate	Maximum allowed rate of BPDUs received per second. (The allowed range of values is from 1 to 10,000.)
burst-size ***bpdus***	Burst tolerance (The allowed range of values is from 1 to 12,500,000.)

1.68.4 Default

No rate limiting is imposed on BPDU traffic in the bridge.

1.68.5 Usage Guidelines

Use the **bpdu rate-limit** command to set the maximum average rate and burst tolerance of received BPDUs.

1.68.6 Examples

The following example shows how to create a spanning tree in the `brdgrp1` bridge and limit the BPDU traffic to `6000` BPDUs received per second and the burst size to `20000` BPDUs:

```
[local]Redback(config)#context isp3
[local]Redback(config-ctx)#bridge brdgrp1
[local]Redback(config-bridge)#spanning-tree
[local]Redback(config-bridge-stp)#bpdu rate-limit 6000 burst-size 20000
```

1.69 bridge

In context configuration mode, the syntax is:

bridge ***bridge-name***

no bridge ***bridge-name***

In interface or subscriber configuration mode, the syntax is:

bridge name ***bridge-name***

In port bvi configuration mode, the syntax is:

bridge name ***bridge-name bvi-context***

1.69.1 Purpose

In context configuration mode, creates a traditional bridge or selects one for modification and enters bridge configuration mode; in interface or subscriber configuration mode, associates the bridge with the interface or subscriber.

1.69.2 Command Mode

- Context configuration
- Interface configuration
- Subscriber configuration
- Port bvi configuration

1.69.3 Syntax Description

bridge-name	Name of the bridge to be created or selected.
name ***bridge-name***	Name of the bridge with which the interface or subscriber is associated.
name ***bridge-name bvi-context***	Context for the BVI port with which the virtual interface is associated.

1.69.4 Default

No bridges are created; no interface or subscriber is associated with any bridge.

1.69.5 Usage Guidelines

In context configuration mode, use the **bridge** command to create a traditional bridge or select one for modification and enter bridge configuration mode; in interface or subscriber configuration mode, use this command to associate the interface or subscriber with a bridge. You can create a bridge either before or after you associate an interfaceor subscriber with it.

Only bridged interfaces can be associated with a bridge; you must create the interface using the **interface** command with the **bridge** keyword (in context configuration mode).

Use the **no** form of this command (in context configuration mode) to delete the bridge.

To configure a Virtual Private LAN Service (VPLS) bridge, see *Configuring VPLS*.

The following sections in *Configuring Bridging* contain closely related information: *Create a Named Bridge*, *Configure a Bridged Interface*, , and *Bridged Virtual Interface Port: Example*.

1.69.6 Examples

The following example shows how to create a bridge, `isp1`:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#bridge isp1
[local]Redback(config-bridge)#
```

The following example shows how to create a bridged interface and associate it with a bridge:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#interface if-isp1 bridge
[local]Redback(config-if)#bridge name isp1
[local]Redback(config-if)#
```

The following example shows how to create a subscriber record and associate it with a bridge:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#subscriber name 9991112222@isp1
[local]Redback(config-if)#bridge name isp1
```

1.70 bridge-mac-address

bridge-mac-address ***mac-addr***

no ***bridge-mac-address***

1.70.1 Purpose

Sets an alias for the bridge MAC address different from the default.

1.70.2 Command Mode

Bridge configuration

1.70.3 Syntax Description

mac-addr	Bridge MAC address in the dotted hexadecimal format ***hh:hh:hh:hh:hh:hh***.

1.70.4 Default

The MAC address of the active controller card

1.70.5 Usage Guidelines

Use the **bridge-mac-address** command to set an alias for the bridge different from the default MAC address.

In the Spanning Tree Protocol, the bridge identifier consists of the bridge MAC address and the bridge priority. Optionally you can set these attributes by the **bridge-mac-address** command and **priority** command (in spanning-tree configuration mode).

1.70.6 Examples

The following example shows how to set the bridge MAC address:

```
[local]Redback(config)#context ink
[local]Redback(config-ctx)#bridge lbdl
[local]Redback(config-bridge)#bridge-mac-address 12:34:56:78:90:ab
```

1.71 bridge mac-entry

bridge mac-entry ***mac-addr***

no bridge mac-entry ***mac-addr***

1.71.1 Purpose

Specifies the medium access control (MAC) address of a station known to be connected to the current PVC, port, or link group.

1.71.2 Command Mode

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

1.71.3 Syntax Description

mac-addr	MAC address of a station that is known to be connected to the current PVC, port, or link group from which source packets are accepted, in the form ***hh:hh:hh:hh:hh:hh***

1.71.4 Default

None

1.71.5 Usage Guidelines

Use the **bridge mac-entry** command to specify the MAC address of a station known to be connected to the current PVC, port, or link group. This MAC address is accepted by the bridge and interface to which the PVC, port, or link group is bound. The bridge dynamically learns the addresses of other stations as they connect to the port.

Use the **no** form of this command to delete the specified MAC address for this circuit.

The following sections in *Configuring Bridging* contain closely related information: *Create a Named Bridge*, *Configure a Bridged Link Group*, and *Bridged Trunk Circuits: Example*.

1.71.6 Examples

The following example shows how to specify the static MAC addresses for an Ethernet port:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#bridge mac-entry 00:d0:ba:04:d8:05
[local]Redback(config-port)#bridge mac-entry 00:0a:0a:04:d8:06
```

1.72 bridge profile

bridge profile {*prof-name* | **default**}

no bridge profile *prof-name*

1.72.1 Purpose

In global configuration mode, creates, or selects for modification, a bridge profile or the default bridge profile, and enters bridge profile configuration mode; in all other modes, assigns an existing bridge profile to a circuit or group of circuits.

1.72.2 Command Mode

- ATM PVC configuration
- dot1q PVC configuration
- Global configuration
- Port configuration
- Subscriber configuration
- Link-group configuration
- VPLS neighbor configuration

1.72.3 Syntax Description

prof-name	Name of the profile to be created, selected, or assigned.
default	Creates or selects the default bridge profile.

1.72.4 Default

No bridge profiles exist or are assigned.

1.72.5 Usage Guidelines

In global configuration mode, use the **bridge profile** command to create, or select for modification, a named bridge profile or the default bridge profile, and enter bridge profile configuration mode; in all other modes, use this command to assign an existing named bridge profile to a circuit or group of circuits.

Use the **default** keyword to create or select the default bridge profile. Each configured attribute in the default profile is included in the configuration for any

circuit that is bound to a bridged interface in any context and that does not have a named bridge profile assigned to it.

Use the ***prof-name*** argument to create a named bridge profile. The configured attributes in the named profile are appended to the configuration for any circuit or group of circuits to which that profile is assigned, and override the attribute values in the default bridge profile.

For subscriber circuits, you can assign a named bridge profile to a default or named subscriber profile or to a subscriber record. When the subscriber circuit is bound to a bridged interface, the attribute values in the named bridge profile assigned to the subscriber record override those in the default bridge profile for the circuit, unless the circuit is also assigned a named bridge profile.

If a named bridge profile is assigned to a circuit or group of circuits, then the attribute values in that named bridge profile override the attribute values in the named bridge profile assigned to the subscriber record.

Use the **no** form of this command to delete the specified bridge profile; you cannot delete the default bridge profile.

1.72.6 Examples

The following example shows how to create a named bridge profile, `prof-isp1`:

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(config-bridge-profile)#
```

The following example shows how to create the `default` bridge profile:

```
[local]Redback(config)#bridge profile default
[local]Redback(config-bridge-profile)#trunk
[local]Redback(config-bridge-profile)#no restricted
[local]Redback(config-bridge-profile)#end
```

1.73 broadcast-discover

broadcast-discover

no broadcast-discover

1.73.1 Purpose

Sends Dynamic Host Configuration Protocol (DHCP) discover packets to other configured servers in a DHCP server group.

1.73.2 Command Mode

DHCP relay server configuration

1.73.3 Syntax Description

This command has no keywords or arguments.

1.73.4 Default

The DHCP client sends discover packets only to the DHCP server in the server group that last responded to the client.

1.73.5 Usage Guidelines

Use the **broadcast-discover** command to send DHCP discover packets to other configured servers in a DHCP server group.

The DHCP relay server always sends initial DHCP discover packets to all DHCP servers in a DHCP server group. By default, it sends subsequent discover packets only to the server that last responded. Servers configured with this command also receive subsequent DHCP discover packets from all clients that have existing sessions with other servers in the group. If the server that last responded to the client is unavailable, another server in the group can respond.

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

1.73.6 Examples

The following example shows how to configure the DHCP relay server, `corp1`, to send DHCP discover packets to all configured servers in the DHCP server group:

```
[local]Redback(config-ctx)#dhcp relay server corp1
[local]Redback(config-dhcp-relay)#broadcast-discover
```

1.74 broadcast rate-limit

broadcast rate-limit {***kbps*** [**burst-size** ***bytes***]}

no broadcast rate-limit

1.74.1 Purpose

Sets the rate and burst tolerance for broadcast traffic on any port, circuit, or Virtual Private LAN Services (VPLS) pseudowire (PW) circuit to which you assign this bridge profile.

1.74.2 Command Mode

Bridge profile configuration

1.74.3 Syntax Description

kbps	Rate, in kilobits per second. The range of values is from 5 to 1,000,000.
burst-size ***bytes***	Burst tolerance in bytes. The range of values is 1 to 12,000,000.

1.74.4 Default

No rate limiting is imposed on broadcast traffic on any port, circuit, or VPLS PW circuit to which you assign this bridge profile.

1.74.5 Usage Guidelines

Use the **broadcast rate-limit** command to set the rate and burst tolerance for broadcast traffic on any port, circuit, or VPLS PW circuit to which this profile is assigned. For more information on VPLS PW circuits, see *Configuring VPLS*.

Use the **no** form of this command to remove any rate limiting for broadcast traffic.

1.74.6 Examples

The following example shows how to create the `prof-isp1` bridge profile and rate limits the broadcast traffic to `6000000` kbps and the burst size to `10000` bytes:

```
[local]Redback(config)#bridge profile prof-isp1
[local]Redback(config-bridge-profile)#broadcast rate-limit 600000 burst-size 10000
```

1.75 bulkstats (IGMP)

bulkstats

no bulkstats

1.75.1 Purpose

Enables IGMP statistics generation on a subscriber circuit.

1.75.2 Command Mode

IGMP service profile configuration

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

IGMP statistics are not generated.

1.75.5 Usage Guidelines

Use the **bulkstats** command to generate statistics on a subscriber circuit within an IGMP service profile.

This command enables bulkstats statistics collection for IGMP. For the IGMP bulkstats feature to work, this option must be enabled within an IGMP service profile and the service profile must be applied to the default subscriber profile.

The bulkstats schema profile and policy are configured independently of this command.

Use the **no** form of this command to disable IGMP statistics generation.

1.75.6 Examples

The following command shows how to enable IGMP statistics generation.

```
[local]Redback(config-ctx)#igmp service-profile test

[local]Redback(config-igmp-service-profile)#bulkstats
```

1.76 bulkstats force transfer

bulkstats force transfer policy ***bulk-pol-name***

1.76.1 Purpose

Immediately transfers the bulk statistics (bulkstats) data file for the specified policy to the configured receiver, rather than waiting for the next transfer interval.

1.76.2 Command Mode

Exec

1.76.3 Syntax Description

policy ***bulk-pol-name***	Name of the bulkstats policy for which a transfer is to be forced.

1.76.4 Default

Bulkstats data is transferred at scheduled intervals.

1.76.5 Usage Guidelines

Use the **bulkstats force transfer** command to immediately transfer the bulkstats file for the specified policy to a configured receiver, rather than waiting for the next transfer interval. Data is transferred to the primary receiver; if this transfer fails, a Simple Network Management Protocol (SNMP) trap is generated and data is transferred to the secondary receiver.

Use the **transfer-interval** command (in bulkstats configuration mode) in the current context to modify the interval at which the SmartEdge router transfers data files to the configured receiver for the specified policy. For more information on the **transfer-interval** command (in bulkstats configuration mode), see *Configuring Bulkstats*.

1.76.6 Examples

The following example shows how to force the bulkstats data file for the `bulk` policy to be transferred immediately to the configured receiver:

```
[local]Redback>bulkstats force transfer policy bulk
```

1.77 bulkstats policy

bulkstats policy ***bulk-pol-name***

no bulkstats policy ***bulk-pol-name***

1.77.1 Purpose

Creates a bulk statistics (bulkstats) policy, or selects one for modification, and enters bulkstats configuration mode.

1.77.2 Command Mode

Context configuration

1.77.3 Syntax Description

bulk-pol-name	Name of the bulkstats policy to be created or modified. Alphanumeric string with up to 19 characters.

1.77.4 Default

None

1.77.5 Usage Guidelines

Use the **bulkstats policy** command to create a bulkstats policy or select one for modification. You can configure multiple bulkstats policies within each context. After creating the policy, add parameters to it with the **collection**, **header**, **limit**, **localdir**, **receiver**, **remotefile**, **sample-interval**, **schema**, **schema-dump**, and **transfer-interval** commands.

For complete syntax and usage guidelines for these commands see the *Command List*.

No more than 100 bulkstats policies are allowed for the entire SmartEdge router.

Caution!

Risk of system performance degradation. Too many bulkstats policies can reduce system performance. To reduce the risk, minimize the number of policies.

Use the **no** form of this command to delete a bulkstats policy.

1.77.6 Examples

The following command shows how to create a bulkstats policy, `bulk`, and enter bulkstats configuration mode:

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

1.78 bulkstats schema

In context or subscriber configuration mode, the syntax is:

bulkstats schema *sch-prof-name* [**policy** *bulk-pol-name* [*ctx-name*]]

no bulkstats schema *sch-prof-name* [**policy** *bulk-pol-name* [*ctx-name*]]

In all other configuration modes listed below, the syntax is:

bulkstats schema *sch-prof-name* [**policy** *bulk-pol-name ctx-name*]

no bulkstats schema *sch-prof-name* [**policy** *bulk-pol-name ctx-name*]

1.78.1 Purpose

Applies an existing bulk statistics (bulkstats) schema profile and bulkstats policy in the specified context to the context, port, channel, or channel group, to a default subscriber profile, or to a profile for an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), Frame Relay PVC, or an 802.1Q PVC.

For Multilink Point-to-Point Protocol (MLPPP) subscribers, data is collected on individual ATM PVC links, as well as the MLPPP bundles.

Note: Bulkstats subscriber schema profiles can only be applied under the default subscriber schema profile.

1.78.2 Command Mode

- ATM OC configuration
- ATM profile configuration
- Context configuration
- Global configuration (for IPsec global level statistics)
- Tunnel configuration
- ASP pool configuration
- dot1q profile configuration
- Frame Relay profile configuration
- IGMP service profile
- Port configuration
- Subscriber configuration

1.78.3 Syntax Description

sch-prof-name	Name of the bulkstats schema profile. Alphanumeric string with up to 19 characters.
policy ***bulk-pol-name***	Optional. Name of the bulkstats policy. Alphanumeric string with up to 19 characters.
ctx-name	Name of the context in which the bulkstats policy is configured. Alphanumeric string with up to 31 characters. Optional in context and subscriber configuration modes.

1.78.4 Default

None

1.78.5 Usage Guidelines

Use the **bulkstats schema** command with the ***ctx-name*** argument (in context and subscriber configuration mode) to allow local context policies to

collect data in other contexts. Applying the name of the context using ***ctx-name*** can only be applied as local in context and subscriber configuration modes.

Use the **bulkstats schema** command, in all other configuration modes, to apply an existing bulkstats schema profile and bulkstats policy in the specified context to the following entities:

- Contexts
- Ports
- Channels or channel groups
- Link groups
- ATM PVC profiles
- Frame Relay PVC profiles
- IGMP service profiles
- 802.1Q PVC profiles
- Default subscriber profiles
- IPsec (global level, tunnel level, asp level)

You can apply multiple bulkstats schema profiles to contexts, ports, channels, channel groups, and profiles using multiple policies in various contexts.

Caution!

Risk of system performance degradation. Although you can apply multiple bulkstats schema profiles that collect different types and formats of data, you should minimize the number of bulkstats schema profile applications to preserve system performance. To reduce the performance impact, create one bulkstats 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 bulkstats schema profile.

Caution!

Risk of system performance degradation. Applying multiple bulkstats policies can reduce system performance. To reduce the risk, minimize the number of policies applied to a port, channel, channel group, or profile.

Note: The SmartEdge 100 router does not support Frame Relay PVCs or 802.1Q PVCs.

Use the **no** form of this command to remove the application of the specified bulkstats schema profile and policy from the context, port, channel, channel group, profile for an 802.1Q PVC, ATM PVC, Frame Relay PVC, or default subscriber profile.

1.78.6 Examples

The following example shows how to apply an existing bulkstats schema profile, `sample`, to an Ethernet port using the `bulk` policy, in the `local` context:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#bulkstats schema sample policy bulk local
```

The following example applies existing bulkstats schema profiles to the context, `isp2`, and to the default subscriber profile in that context, using the `bulk-isp2` policy:

```
[local]Redback(config)#context isp2
[local]Redback(config-ctx)#bulkstats schema ctx-sample policy bulk-isp2
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#bulkstats schema sub-sample policy bulk-isp2
```

1.79 bulkstats schema profile

bulkstats schema profile ***prof-type sch-prof-name*** {**format** ***format-string*** [***OS-variable***] [***OS-variable***] ***...***}

no bulkstats schema profile ***prof-type sch-prof-name***

1.79.1 Purpose

Creates or modifies a bulkstats schema profile that can be used to collect statistics system-wide, or for contexts, subscribers, ports, channels, or Asynchronous Transfer Mode (ATM), Frame Relay, 802.1Q permanent virtual circuits (PVCs), IGMP service profiles, or media gateways, or IPsec at tunnel, asp and global level.

1.79.2 Command Mode

Global configuration

1.79.3 Syntax Description

prof-type	Type of bulkstats profile according to one of the keywords listed in Table 11.
sch-prof-name	Name of the bulkstats schema profile to be defined.
format ***format-string***	Table 12 describes the format strings used to format the bulkstats schema profile. Format strings can contain anything or nothing as a label for an operating system variable. They follow the C programming language printf() function syntax and must be enclosed in quotation marks.
OS-variable	Optional. Operating system variable for which data is collected. Separate the variables with a space. Table 13 to to Table 24 describe the supported operating system variables for different types of bulkstats schema profiles.

1.79.4 Default

No bulkstats schema profile is defined.

1.79.5 Usage Guidelines

Use the **bulkstats schema profile** command to create or modify a bulkstats schema profile that can be used as a template to gather statistics system-wide or for contexts, subscribers, ports, channels, ATM, Frame Relay, 802.1Q PVCs, or media gateways, or IPsec at tunnel, ASP, and global level.

Table 11 lists the keywords for the types of bulkstats schema profiles that you can create or modify.

Table 11 Types of Bulkstats Schema Profiles

Keyword	Description	Relevant Statistics Variables
atm	ATM PVCs (using ATM profiles).	Table 18
context	One or more contexts.	Table 14
dot1q	One or more 802.1Q PVCs (using dot1q profiles).	Table 21
frame-relay	One or more Frame Relay PVCs (using Frame Relay profiles).	Table 19
global	System-wide statistics.	Table 13
link-group	One or more link groups.	Table 22
igmp	IGMP service profile.	Table 20

Table 11 Types of Bulkstats Schema Profiles

Keyword	Description	Relevant Statistics Variables
ipsec tunnel	IPsec statistics at the tunnel level.	Table 26
ipsec global	IPsec statistics at the global level.	Table 25
ipsec asp	IPsec statistics at the ASP level.	Table 27
media-gateway global	Media-gateway statistics at the global level.	Table 23
media-gateway mgc-group	Media gateway statistics at the MGC group level.	Table 24
port	One or more ATM or Packet over SONET/SDH (POS) ports.	Table 16
subscriber	One or more subscribers (using default subscriber profiles).	Table 15

To apply a global bulkstats schema profile to the system, use the **schema** command in bulkstats configuration mode.

To apply a bulkstats schema profile to a context, port, channel, or PVC, use the **bulkstats schema** command in the appropriate configuration mode.

To apply a bulkstats schema profile to a default subscriber profile, use the **bulkstats schema** command with the **apply** keyword in subscriber configuration mode.

To save the definitions of a bulkstats schema profiles in the collection file, use the **schema-dump** command in bulkstats configuration mode.

Note: The SmartEdge 100 router does not support Frame Relay PVCs or 802.1Q PVCs.

Use the **no** form of this command to delete the specified bulkstats schema profile. When you delete a schema profile, all the references (applications) of the profile are also removed. If the same statistics are to be collected, the schema profile must be recreated and reapplied.

Table 12 describes the supported format strings.

Table 12 Format String Special Character Descriptions

Syntax	Description
\n	Creates a new line
%s	Represents a character string
%d	Represents an integer in decimal (base 10)

Syntax	Description
%u	Represents an unsigned integer in decimal (base 10)
%llu	Represents a Counter64 type non-negative integer
%x	Represents an integer in hexadecimal format (base 16)
%%	Represents a single % character in the output

Caution!

Risk of system performance degradation. Although you can apply multiple bulkstats schema profiles, each gathering a different type and format of data, it is advisable to minimize the number of bulkstats schema profile applications to reduce impact on system performance. To reduce the risk, you can instead create one bulkstats 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 bulkstats schema profile in place of multiple bulkstats schema profiles.

Caution!

Risk of system performance degradation. Schema profiles that are created with policing and drop counters (the qos_inoctets, qos_outoctets, rcv_drop_octets, xmt_drop_octets variables) could result in a substantial increase in CPU usage, when applied, using the **bulkstats schema** command in any of its configuration modes). To reduce the risk, limit their use whenever possible or decrease the sampling rate (by increasing the sample interval using the **sample-interval** command in bulkstats configuration mode) when the bulkstats schema with these parameters is applied to a large number of ports, channels, or circuits.

Table 13 describes the supported SmartEdge OS variables for bulkstats global schema profiles.

Table 13 SmartEdge OS Variables for Bulkstats Global Schema Profiles

Variable	Description	Type	Value	MIB Mapping
active_subs	Number of active subscribers	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtCount
active_dualStack_subs	Number of active subscribers enabled for both IPv4 and IPv6	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtDualCount
active_ipv4_subs	Number of active subscribers enabled for IPv4	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtIp4Only
active_ipv6_subs	Number of active subscribers enabled for IPv6	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtIp6Only
active_subs_bridged1483	Number of active subscribers on RFC 1483-bridged circuits	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.3
active_subs_CLIPS	Number of active subscribers on CLIPS circuits	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.12
active_subs_dot1qEnet	Number of active subscribers on 802.1Q PVCs	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.7
active_subs_ppp	Number of active subscribers on PPP-encapsulated circuits	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.1
active_subs_pppoe	Number of active subscribers on PPPoE-encapsulated circuits	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.2
active_subs_routed1483	Number of active subscribers on RFC 1483-routed circuits	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.4
cpu1min	System CPU usage for the last minute	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnCpuMeterOneMinuteAvg

Table 13 SmartEdge OS Variables for Bulkstats Global Schema Profiles

Variable	Description	Type	Value	MIB Mapping
cpu5min	System CPU usage for the last 5 minutes	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnCpuMeterFiveMinuteAvg
cpu5sec	System CPU usage for the last 5 seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnCpuMeterFiveSecondAvg
date	The date today in yyyy/mm/dd format	String	Date in YYYYMMDD > format	RbnSRSystemDate
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
free_user_mem	Available memory in KB	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnMemoryFreeKBytes
hostname	System hostname	String	64 characters	SysName
load15min	System load average for the last 15 minutes	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
load1min	System load average for the last minute	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
load5min	System load average for the last 5 minutes	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime

Table 13 SmartEdge OS Variables for Bulkstats Global Schema Profiles

Variable	Description	Type	Value	MIB Mapping
timeofday	Time of day in hhmmss format using a 24-hour clock	String	Time in HHMMSS format	RbnSRSystemDate
total_user_mem	Total memory in KB	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnMemoryFreeKBytes and rbnMemoryKBytesInUse

Table 14 describes the supported SmartEdge OS variables for bulkstats context schema profiles.

Table 14 SmartEdge OS Variables for Bulkstats Context Schema Profiles

Variable	Description	Type	Value	MIB Mapping
active_subs	Active subscribers for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSubsCntxtCount
active_dualStack_subs	Number of active subscribers enabled for both IPv4 and IPv6 for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtDualCount
active_ipv4_subs	Number of active subscribers enabled for IPv4 for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtIp4Only
active_ipv6_subs	Number of active subscribers enabled for IPv6 for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsCntxtIp6Only
active_subs_bridged1483	Active subscribers on RFC 1483-bridged circuits for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.3
active_subs_clips	Active subscribers on CLIPS circuits for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.12
active_subs_dot1qEnet	Active subscribers on 802.1Q PVCs for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.7

Table 14 SmartEdge OS Variables for Bulkstats Context Schema Profiles

Variable	Description	Type	Value	MIB Mapping
active_subs_ppp	Active subscribers on PPP-encapsulated circuits for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.1
active_subs_pppoe	Active subscribers on PPPoE-encapsulated circuits for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.2
active_subs_routed1483	Active subscribers on RFC 1483-routed circuits for this context	Integer Absolute Value	Unsigned32 0 - 4294967295	RbnSubsEncapsCount.4
context_name	Context name	String	64 characters	vacmContextName
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime

Table 15 describes the supported SmartEdge OS variables for bulkstats subscriber schema profiles.

Table 15 SmartEdge OS Variables for Subscriber Schema Profiles

Variable	Description	Type	Value	MIB Mapping
agent_circuit_id	Agent circuit ID corresponding to this subscriber.	String	64 characters	N/A
agent_remote_id	Agent remote ID corresponding to this subscriber.	String	64 characters	N/A
bind_type	Subscriber bind type.	String	80 characters	RbnBindType
cct_handle	Circuit descriptor.	String	64 characters	rbnSubsActiveCircuitHandle

Table 15 SmartEdge OS Variables for Subscriber Schema Profiles

Variable	Description	Type	Value	MIB Mapping
context_name	Context name.	String	64 characters	vacmContextName
epochtime	Time of day in epoch format (number of seconds since January 1, 1970).	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsOctetsReceived
inpackets	Number of packets received on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsPktsReceived
ip_addr	IP address.	String	32 characters	rbnSubsActiveAddr
ip_mask	IP address mask.	String	32 characters	N/A
mcast_inoctets	Number of multicast octets received on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsMcastOctetsReceived
mcast_inpackets	Number of multicast packets received on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsMcastPktsReceived
mcast_outoctets	Number of multicast octets sent on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsMcastOctetsSent
mcast_outpackets	Number of multicast packets sent on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsMcastPktsSent

Table 15 SmartEdge OS Variables for Subscriber Schema Profiles

Variable	Description	Type	Value	MIB Mapping
metering_class_counters	Metering counter statistics for each Differentiated Services Code Point (DSCP) class for this subscriber session. One line of output exists for each class defined in the corresponding QoS metering policy.	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosSubscriberRLClassStatsEntry
metering_policy_name	Names of the QoS metering policy applied to this subscriber.	String	64 characters	rbnQosSubsRLPolicyName
num_queues	Number of queues configured on this subscriber session.	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
outoctets	Number of octets sent on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsOctetsSent
outpackets	Number of packets sent on this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	rbnSubsPktsSent
policing_class_counters	Policing counter statistics for each DSCP class for this subscriber session. Each class defined in the corresponding QoS policing policy has a line of output..	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosSubscriberRLClassStatsEntry
policing_policy_name	Name of the QoS policing policy applied to this subscriber.	String	40 characters	rbnQosSubsRLPolicyName
queue_counters	Number of queue counters for this subscriber session.	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosSubscriberQueueStatsEntry

Table 15 SmartEdge OS Variables for Subscriber Schema Profiles

Variable	Description	Type	Value	MIB Mapping
queue_policy_name	QoS PWFQ policy name.	String	40 characters	rbnQosSubsQueuePolicyName
session_id	Subscriber session ID.	String	29 characters	rbnSubsActiveSessionId
start_time	Session start time in seconds.	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSubsActiveStartTime
sysuptime	System uptime in seconds.	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
user_name	Username.	String	254 characters	rbnSubsActiveName

Note: Configuring the `agent_remote_id` variable in the bulkstats subscriber schema profile causes the output data to contain the string value in the configuration.

Configuring the `agent_circuit_id` variable in the bulkstats subscriber schema profile causes the output data to contain the string value in the configuration.

Application of the bulkstats subscriber schema to the default bulkstats subscriber profile for a context affects all subscribers in the context.

Note: Configuring the queue_counters variable in the bulkstats subscriber schema profiles causes the output data to contain the queue counter statistics, when applicable. If no quality of service (QoS) priority weighted fair queuing (PWFQ) policy is applied, the queue_counters variable displays an error message.

One line is printed for each queue. Each line contains a predefined format, with all the following elements (none are configurable) and can contain up to 16,384 bits:

- queue_index
- outoctets
- outpackets
- wred_drop_octets
- wred_drop_packets
- tail_drop_octets
- tail_drop_packets

Note: Configuring the metering_class_counters or the policing_class_counters variable in the bulkstats subscriber schema profile causes the output data to contain the counter statistics for each class, when applicable.

Application of the bulkstats subscriber schema to the default subscriber profile for a context affects all subscribers in the context.

One line of output data is printed for each class, each containing a predefined format with all of the following elements (none are configurable) and can contain up to 16,384 bits:

- class_name
- conform_octets
- conform_packets
- conform_drop_octets
- conform_droppackets
- exceed_octets
- exceed_packets
- exceed_drop_octets
- exceed_drop_packets
- violate_octets
- violate_packets
- violate_drop_octets
- violate_drop_packets

If no QoS policy is applied, the output line for the metering_class_counters parameter or the policing_class_counters parameter displays `N/A`.

Table 16 describes the supported SmartEdge router variables for bulkstats port schema profiles.

Table 16 SmartEdge OS Variables for Bulkstats Port Schema Profiles

Variable	Description	Type	Value	MIB Mapping
description	Description of the port	String	256 characters	ifAlias
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A

Table 16 SmartEdge OS Variables for Bulkstats Port Schema Profiles

Variable	Description	Type	Value	MIB Mapping
inoctets	Number of octets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	ifInOctets
inpackets	Number of packets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	ifInUcastPkts
mcast_inoctets	Number of multicast octets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_inpackets	Number of multicast packets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	ifInMulticastPkts
mcast_outoctets	Number of multicast octets sent on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_outpackets	Number of multicast packets sent on this port	Integer Counter	Counter64 0 - 18446744073709551615	ifOutMulticastPkts
metering_class_counters	Packet statistics, class-based metering on this port, one line of output for each DSCP class defined in the metering policy.	String	92...640 bytes	RbnQosIntfRLClassStatsEntry
metering_policy_name	Name of the QoS metering policy applied to the port	String	40 characters	rbnQosIfRLPolicyName
outoctets	Number of octets sent on the port	Integer Counter	Counter64 0 - 18446744073709551615	ifOutOctets
outpackets	Number of packets sent on the port	Integer Counter	Counter64 0 - 18446744073709551615	ifOutUcastPkts

Table 16 SmartEdge OS Variables for Bulkstats Port Schema Profiles

Variable	Description	Type	Value	MIB Mapping
policing_class_counters	Packet statistics, class-based policing on this port, one line of output for each DSCP class defined in the policing policy	String	183...1280 bytes	RbnQosIntfRLClassStatsEntry
policing_policy_name	Name of the QoS policing policy applied to the port	String	40 characters	rbnQosIfRLPolicyName
port	Port number on the line card	Integer Absolute Value	Unsigned32 0 - 4294967295	ifDescr (port eth 4/1)
portspeed	Port speed in kbps	Integer Absolute Value	Unsigned32 0 - 4294967295	ifSpeed
porttype	Port type	String	32 characters	ifType
qos_inoctets	Number of post-limited octets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
rcv_drop_octets	Number of receive octets dropped on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
slot	Slot number in the SmartEdge router(1)	Integer Absolute Value	Unsigned32 0 - 4294967295	ifDescr (port eth 4/1)
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
xmt_drop_octets	Number of transmitted octets dropped on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A

(1) On the SmartEdge 100 router, only slot 2 interfaces to subscriber sessions.

Table 17 describes the supported SmartEdge OS variables for bulkstats channel schema profiles.

Table 17 SmartEdge OS Variables for Bulkstats Channel Schema Profiles

Variable	Description	Type	Value	MIB Mapping
channelCircuit	Circuit descriptor for the channel.	String	Channel (slot, port, channel) Subchannel (slot, port, channel, subchannel) or Subsubchannel (slot, port, channel, subchannel, sub-subchannel)	ifName
channel	Channel number on port	Integer Absolute Value	Unsigned32 0 - 4294967295	IfName/ifDescr
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on this channel	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInOctets
inpackets	Number of packets received on this channel	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInUcastPkts
mcast_inoctets	Number of multicast octets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_inpackets	Number of multicast packets received on this port	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInMulticastPkts
mcast_outoctets	Number of multicast octets sent on this port	Integer Counter	Counter64 0 - 18446744073709551615	N/A

Table 17 SmartEdge OS Variables for Bulkstats Channel Schema Profiles

Variable	Description	Type	Value	MIB Mapping
mcast_outpackets	Number of multicast packets sent on this port	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutMulticastPkts
outoctets	Number of octets sent on this channel	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutOctets
outpackets	Number of packets sent on this channel	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutUcastPkts
port	Port number on the line card	Integer Absolute Value	Unsigned32 0 - 4294967295	IfName/ifDescr
qos_inoctets	Number of post-limited octets received on this channel	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on this channel	Integer Counter	Counter64 0 - 18446744073709551615	N/A
rcv_drop_octets	Number of receive octets dropped on this channel	Integer Counter	Counter64 0 - 18446744073709551615	N/A
slot	Slot number in the SmartEdge router(1)	Integer Absolute Value	Unsigned32 0 - 4294967295	IfName/ifDescr
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
xmt_drop_octets	Number of transmitted octets dropped on this channel	Integer Counter	Counter64 0 - 18446744073709551615	N/A

(1) On the SmartEdge 100 router, only slot 2 interfaces to subscriber sessions.

Table 18 describes the supported SmartEdge OS variables for bulkstats ATM PVC schema profiles.

Table 18 SmartEdge OS Variables for Bulkstats ATM PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
cctstate	State of the ATM PVC	String	UP/DOWN	ifOperStatus
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInOctets
inpackets	Number of packets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInUcastPkts
mcast_inoctets	Number of multicast octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_inpackets	Number of multicast packets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInMulticastPkts
mcast_outoctets	Number of multicast octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_outpackets	Number of multicast packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutMulticastPkts
metering_class_counters	Packet statistics, class-based metering on this PVC, one line of output for each DSCP class defined in the metering policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry
metering_policy_name	Name of the QoS metering policy applied to the PVC	String	40 characters	rbnQosIfRLPolicyName

Table 18 SmartEdge OS Variables for Bulkstats ATM PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
outoctets	Number of octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutOctets
outpackets	Number of packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutUcastPkts
policing_class_counters	Packet statistics, class-based policing on this PVC, one line of output for each DSCP class defined in the policing policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry
policing_policy_name	Name of the QoS policing policy applied to the PVC	String	40 characters	rbnQosIfRLPolicyName
port	Port number on the line card	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr
qos_inoctets	Number of post-limited octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
rcv_drop_octets	Number of receive octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
slot	Slot number in the SmartEdge router(1)	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
vci	Virtual channel identifier (VCI) for the PVC	Integer Absolute Value	Unsigned32 0 - 4294967295	ifDescr/ifName

Table 18 SmartEdge OS Variables for Bulkstats ATM PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
vpi	Virtual path identifier (VPI) for the PVC	Integer Absolute Value	Unsigned32 0 - 4294967295	ifDescr/ifName
xmt_drop_octets	Number of transmitted octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A

(1) On the SmartEdge 100 router, only slot 2 interfaces to subscriber sessions.

Table 19 describes the supported SmartEdge OS variables for bulkstats Frame Relay PVC schema profiles.

Table 19 SmartEdge OS Variables for Frame Relay PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
cctstate	State of the Frame Relay PVC	String	UP/DOWN	ifOperStatus
channel	Channel number on the port	Integer Absolute Value	Unsigned32 0 - 4294967295	IfName/ifDescr
dlci	Data-link connection identifier (DLCI) for the PVC	Integer Absolute Value	Unsigned32 0 - 4294967295	IfName/ifDescr
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInOctets
inpackets	Number of packets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInUcastPkts
mcast_inoctets	Number of multicast octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A

Table 19 SmartEdge OS Variables for Frame Relay PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
mcast_inpackets	Number of multicast packets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInMulticastPkts
mcast_outoctets	Number of multicast octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_outpackets	Number of multicast packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutMulticastPkts
outoctets	Number of octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutOctets
outpackets	Number of packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutUcastPkts
port	Port number on the line card	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr
qos_inoctets	Number of post-limited octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
rcv_drop_octets	Number of receive octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
slot	Slot number in the SmartEdge router(1)	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr

Table 19 SmartEdge OS Variables for Frame Relay PVC Schema Profiles

Variable	Description	Type	Value	MIB Mapping
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
xmt_drop_octets	Number of transmitted octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A

(1) On the SmartEdge 100 router, only slot 2 interfaces to subscriber sessions.

Table 20 describes the supported SmartEdge OS variables for bulkstats IGMP schema profiles. Note that for bulkstat profiles to be brought into effect, the schema must be applied to an IGMP service profile configured under the subscriber default profile. Note also that format strings are not supported for IGMP schema profiles.

Table 20 SmartEdge OS Variables for IGMP Service Profiles

Variable /Code	Type	Event/Statistic Description
Session IP Address	IP address	When the generation of statistics on the circuit begins, the source address of the first host on the session is stored. This address does not change until the session terminates.
ID	ID	The remote agent ID is recorded when the subscriber first connects. The remote agent ID is an identifier that uniquely identifies each subscriber. It is obtained from the ISM process.
1	Integer Counter	The IGMP module on the router received an IGMP Leave message for the specified group. The event includes the group address.
17	Integer Counter	The IGMP module on the router received no response to a query. This event occurs when the IGMP group on the circuit times out and the group is deleted. The event includes the group address.
54	Integer Counter	The IGMP module on the router rejected a response due to insufficient bandwidth at the service virtual local area network (S-VLAN). This event occurs when the IGMP group on the circuit times out and the group is delete when an IGMP report is not processed because of insufficient bandwidth on the circuit. The event includes the group address.

Table 20 SmartEdge OS Variables for IGMP Service Profiles

Variable /Code	Type	Event/Statistic Description
55	Integer Counter	The IGMP module on the router rejected a response due to exceeding the maximum number of groups. This event occurs when the IGMP group on the circuit times out and the group is delete when an IGMP report is not processed because the maximum number of groups on the circuit has already been reached. The event includes the group address.
57	Integer Counter	The IGMP module on the router rejected a response due to invalid IGMPv3 source address. This event occurs when the IGMP group on the circuit times out and the group is delete when an IGMP report is not processed because the source address in the IGMPv3 report is not valid. The event includes the source address.
71/72	Integer Counter	Indicates whether the subscriber is enabled for Remote Multicast Replication (RMR) quality of service (QoS) or whether or whether it receives traffic through replication at the router. Supported values are as follows: 71: RMR QoS is enabled on the subscriber. 72: Replication occurs locally at the router.
73	Integer Counter	The IGMP module on the router rejected a response due to invalid groups. This event occurs when the IGMP group on the circuit times out and the group is delete when an IGMP report is not processed because the IGMP group in the report is not valid. The event includes the group address.
74	Integer Counter	The IGMP module on the router received an IGMP Join message for the group. For IGMPv2, this code and the group address are stored whenever an IGMPv2 report is received from the host.
75	Integer Counter	The IGMP module on the router received an IGMPv3 MODE_IS_INCLUDE message for the specified group. IGMPv3 messages can be sent to multiple groups or sources. In this case, multiple records are generated: one for each group/source combination. The event includes the group address plus the list of source addresses.
76	Integer Counter	The IGMP module on the router received an IGMPv3 MODE_IS_EXCLUDE message for the specified group. The event includes the group address plus the list of source addresses.
77	Integer Counter	The IGMP module on the router received an IGMPv3 CHANGE_TO_INCLUDE_MODE message for the specified group. The event includes the group address plus the list of source addresses.

Table 20 SmartEdge OS Variables for IGMP Service Profiles

Variable /Code	Type	Event/Statistic Description
78	Integer Counter	The IGMP module on the router received an IGMPv3 CHANGE_TO_EXCLUDE_MODE message for the specified group. The event includes the group address plus the list of source addresses.
79	Integer Counter	The IGMP module on the router received an IGMPv3 ALLOW_NEW_SOURCES message for the specified group. The event includes the group address plus the list of source addresses.
80	Integer Counter	The IGMP module on the router received an IGMPv3 BLOCK_OLD_SOURCES message for the specified group. The event includes the group address plus the list of source addresses.
81	Integer Counter	This code is generated when the statistics buffer reaches capacity and wraps around. This can occur with a maximum number of entries, or when the buffer grows to a maximum size and statistics have not been queried. After the buffer wraps around, the oldest entries are replaced by the new entries.
88	Integer Counter	Indicates the sources present in the IGMPv3 report. The event includes the group address plus the list of source addresses.

Table 21 describes the supported SmartEdge router variables for bulkstats 802.1Q PVC (dot1q) schema profiles.

Table 21 SmartEdge OS Variables for Bulkstats 802.1Q PVC (dot1q) Schema Profiles

Variable	Description	Type	Value	MIB Mapping
cctstate	State of the 802.1Q PVC	String	UP/DOWN	ifOperStatus
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on the PVC	Integer Counter	Counter64 0 - 18446744073 709551615	IfHCInOctets
inpackets	Number of packets received on the PVC	Integer Counter	Counter64 0 - 18446744073 709551615	IfHCInUcastPkts

Table 21 SmartEdge OS Variables for Bulkstats 802.1Q PVC (dot1q) Schema Profiles

Variable	Description	Type	Value	MIB Mapping
mcast_inoctets	Number of multicast octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_inpackets	Number of multicast packets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInMulticastPkts
mcast_outoctets	Number of multicast octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_outpackets	Number of multicast packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutMulticastPkts
metering_class_counters	Packet statistics, class-based metering on this PVC, one line of output for each DSCP class defined in the metering policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry
metering_policy_name	Name of the QoS metering policy applied to the PVC	String	40 characters	rbnQosIfRLPolicyName
outoctets	Number of octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutOctets
outpackets	Number of packets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutUcastPkts
policing_class_counters	Packet statistics, class-based policing on this PVC, one line of output for each DSCP class defined in the policing policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry

Table 21 SmartEdge OS Variables for Bulkstats 802.1Q PVC (dot1q) Schema Profiles

Variable	Description	Type	Value	MIB Mapping
policing_policy_name	Name of the QoS policing policy applied to the PVC	String	40 characters	rbnQosIfRLPolicyName
port	Port number on the line card	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr
qos_inoctets	Number of post-limited octets received on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
rcv_drop_octets	Number of receive octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A
slot	Slot number in the SmartEdge router (1)	Integer Absolute Value	Unsigned32 0 - 4294967295	ifName/ifDescr
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
vlan_id	VLAN tag value for the PVC	String	20 characters	ifDescr/ifName
xmt_drop_octets	Number of transmitted octets dropped on the PVC	Integer Counter	Counter64 0 - 18446744073709551615	N/A

(1) On the SmartEdge 100 router, only slot 2 interfaces to subscriber sessions.

Table 22 describes the supported SmartEdge OS variables for bulkstats link-group schema profiles.

Table 22 SmartEdge OS Variables for Bulkstats Link-group Schema Profiles

Variable	Description	Type	Value	MIB Mapping
description	Name of link-group	String	17 characters	IfName

Table 22 SmartEdge OS Variables for Bulkstats Link-group Schema Profiles

Variable	Description	Type	Value	MIB Mapping
linkgrouptype	Type of link-group; one of the following: DOT1Q LINK-GROUP MP LINK-GROUP *(Note: MLPPP link group)* ETHER LINK-GROUP ACCESS LINK-GROUP UNSUPPORTED LINK-GROUP	String	21 characters	ifType
epochtime	Time of day in epoch format (number of seconds since January 1, 1970)	Integer Absolute Value	Unsigned32 0 - 4294967295	N/A
inoctets	Number of octets received on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInOctets
inpackets	Number of packets received on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInUcastPkts
mcast_inoctets	Number of multicast octets received on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A
mcast_inpackets	Number of multicast packets received on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCInMulticastPkts
mcast_outoctets	Number of multicast octets sent on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A

Table 22 SmartEdge OS Variables for Bulkstats Link-group Schema Profiles

Variable	Description	Type	Value	MIB Mapping
mcast_outpackets	Number of multicast packets sent on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutMulticastPkts
metering_class_counters	Packet statistics, class-based metering on this link group, one line of output for each DSCP class defined in the metering policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry
metering_policy_name	Name of the QoS metering policy applied to the link group	String	40 characters	rbnQosIfRLPolicyName
outoctets	Number of octets sent on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutOctets
outpackets	Number of packets sent on the link group	Integer Counter	Counter64 0 - 18446744073709551615	IfHCOutUcastPkts
policing_class_counters	Packet statistics, class-based policing on this link group, one line of output for each DSCP class defined in the policing policy	Integer Counter	Counter64 0 - 18446744073709551615	RbnQosIntfRLClassStatsEntry
policing_policy_name	Name of the QoS policing policy applied to the link group	String	40 characters	rbnQosIfRLPolicyName
qos_inoctets	Number of post-limited octets received on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A
qos_outoctets	Number of prelimited octets sent on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A

Table 22 SmartEdge OS Variables for Bulkstats Link-group Schema Profiles

Variable	Description	Type	Value	MIB Mapping
rcv_drop_octets	Number of receive octets dropped on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A
sysuptime	System uptime in seconds	Integer Absolute Value	Unsigned32 0 - 4294967295	rbnSRSystemUptime
xmt_drop_octets	Number of transmitted octets dropped on the link group	Integer Counter	Counter64 0 - 18446744073709551615	N/A

Table 23 describes the supported SmartEdge OS variables for bulkstats media-gateway schema profiles at the global level.

Note: MIB mappings for bulkstats global media-gateway schema profiles do not exist.

Table 23 SmartEdge OS Variables for Bulkstats Global Media-Gateway Schema Profiles

Variable	Description	Type	Value
current_calls	Number of current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
normal_current_calls	Number of normal current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
emergency_current_calls	Number of emergency current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
peak_calls	Number of peak calls	Integer Absolute Value	Unsigned32 0 - 4294967295
emergency_peak_calls	Number of emergency peak calls	Integer Absolute Value	Unsigned32 0 - 4294967295
current_streams	Number of current streams	Integer Absolute Value	Unsigned32 0 - 4294967295

Table 23 SmartEdge OS Variables for Bulkstats Global Media-Gateway Schema Profiles

Variable	Description	Type	Value
v4_v4_current_streams	Number of IPv4 - IPv4 current streams	Integer Absolute Value	Unsigned32 0 - 4294967295
v4_v6_current_streams	Number of IPv4 – IPv6 current streams	Integer Absolute Value	Unsigned32 0 - 4294967295
v6_v6_current_streams	Number of IPv6 – IPv6 current streams	Integer Absolute Value	Unsigned32 0 - 4294967295
peak_streams	Number of peak streams	Integer Absolute Value	Unsigned32 0 - 4294967295
v4_v4_peak_streams	Number of IPv4 - IPv4 peak streams	Integer Absolute Value	Unsigned32 0 - 4294967295
v4_v6_peak_streams	Number of IPv4 – IPv6 peak streams	Integer Absolute Value	Unsigned32 0 - 4294967295
v6_v6_peak_streams	Number of IPv6 – IPv6 peak streams	Integer Absolute Value	Unsigned32 0 - 4294967295
reject_emergency_threshold	Total number of rejections due to Emergency Threshold	Integer Counter	Counter64 0 - 18446744073709551615
reject_license	Total number of rejections due to Licensing Limit	Integer Counter	Counter64 0 - 18446744073709551615
reject_stream	Total number of rejections due to Stream Limit	Integer Counter	Counter64 0 - 18446744073709551615
reject_bandwidth	Total number of rejections due to Bandwidth Limit	Integer Counter	Counter64 0 - 18446744073709551615

Table 23 SmartEdge OS Variables for Bulkstats Global Media-Gateway Schema Profiles

Variable	Description	Type	Value
reject_insuff_resources	Total number of rejections due to Insufficient Resources	Integer Counter	Counter64 0 - 18446744073 709551615
reject_routing_failures	Total number of rejections due to Routing Failures	Integer Counter	Counter64 0 - 18446744073 709551615
add_avg_latency	Average Latency for H.248 ADD message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
modify_avg_latency	Average Latency for H.248 MODIFY message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
subtract_avg_latency	Average Latency for H.248 SUBTRACT message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
add_peak_latency	Peak Latency for H.248 ADD message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
modify_peak_latency	Peak Latency for H.248 MODIFY message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
subtract_peak_latency	Peak Latency for H.248 SUBTRACT message (ms)	Integer Absolute Value	Unsigned32 0 - 4294967295
throttle_active	Throttle active	string	Possible values: Yes, No
throttle_state	Throttle state	string	Possible values: T0, T1, T2
t1_throttled	Total number of calls throttled in T1 state	Integer Counter	Counter64 0 - 18446744073 709551615
t2_throttled	Total number of calls throttled in T2 state	Integer Counter	Counter64 0 - 18446744073 709551615

Table 23 SmartEdge OS Variables for Bulkstats Global Media-Gateway Schema Profiles

Variable	Description	Type	Value
current_cps_accepted	Accepted current CPS (calls per second)	Integer Absolute Value	Unsigned32 0 - 4294967295
avg_cps_accepted	Accepted average CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
min_cps_accepted	Accepted minimum CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
max_cps_accepted	Accepted maximum CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
current_cps_rejected	Rejected current CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
avg_cps_rejected	Rejected average CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
min_cps_rejected	Rejected minimum CPS	Integer Absolute Value	Unsigned32 0 - 4294967295
max_cps_rejected	Rejected maximum CPS	Integer Absolute Value	Unsigned32 0 - 4294967295

Table 24 describes the supported SmartEdge OS variables for bulkstats media-gateway schema profiles at the mgc-group level.

Note: MIB mappings for bulkstats global media-gateway schema profiles do not exist.

Table 24 SmartEdge OS Variables for Bulkstats MGC-Group Media-Gateway Schema Profiles

Variable	Description	Type	Value
mgc_group_name	MGC-Group name	string	Up to 19 characters.

Table 24 SmartEdge OS Variables for Bulkstats MGC-Group Media-Gateway Schema Profiles

Variable	Description	Type	Value
assoc_state	Association State	string	Possible values: null, connected, disconnected
transport	Transport used to connect with current active MGC	string	Possible values: sctp, udp, tcp
local_address	Local address used to connect with current active MGC	TBD ?	IP:Port
remote_address	Remote address of current active MGC	TBD ?	IP:Port
current_calls	Number of current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
normal_current_calls	Number of normal current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
emergency_current_calls	Number of emergency current calls	Integer Absolute Value	Unsigned32 0 - 4294967295
peak_calls	Number of peak calls	Integer Absolute Value	Unsigned32 0 - 4294967295
normal_peak_calls	Number of normal peak calls	Integer Absolute Value	Unsigned32 0 - 4294967295
emergency_peak_calls	Number of emergency peak calls	Integer Absolute Value	Unsigned32 0 - 4294967295
current_media_flows	Number of current media flows	Integer Absolute Value	Unsigned32 0 - 4294967295
current_active_media_flows	Number of current active media flows	Integer Absolute Value	Unsigned32 0 - 4294967295

Table 24 SmartEdge OS Variables for Bulkstats MGC-Group Media-Gateway Schema Profiles

Variable	Description	Type	Value
peak_active_media_flows	Number of peak active media flows	Integer Absolute Value	Unsigned32 0 - 4294967295
cumulative_total_media_flows	Number of cumulative total media flows	Integer Counter	Counter64 0 - 18446744073709551615
reject_emergency_threshold	Total number of rejections due to emergency threshold	Integer Counter	Counter64 0 - 18446744073709551615
reject_license	Total number of rejections due to licensing limit	Integer Counter	Counter64 0 - 18446744073709551615
reject_stream	Total number of rejections due to stream limit	Integer Counter	Counter64 0 - 18446744073709551615
reject_bandwidth	Total number of rejections due to bandwidth limit	Integer Counter	Counter64 0 - 18446744073709551615
reject_insuff_resources	Total number of rejections due to insufficient resources	Integer Counter	Counter64 0 - 18446744073709551615
reject_routing_failures	Total number of rejections due to Routing Failures	Integer Counter	Counter64 0 - 18446744073709551615
hangterm_notifications	Total number of hangterm notifications	Integer Counter	Counter64 0 - 18446744073709551615
idle_media_flows	Total number of idle media flows	Integer Counter	Counter64 0 - 18446744073709551615
used_bandwidth	Used bandwidth (bytes/sec)	Integer Counter	Counter64 0 - 18446744073709551615

Table 24 SmartEdge OS Variables for Bulkstats MGC-Group Media-Gateway Schema Profiles

Variable	Description	Type	Value
used_packet_rate	Used packet rate	Integer Counter	Counter64 0 - 18446744073709551615
media_packets_received	Total number of media packets received	Integer Counter	Counter64 0 - 18446744073709551615
media_packets_sent	Total number of media packets sent	Integer Counter	Counter64 0 - 18446744073709551615
media_packets_dropped	Total number of media packets dropped	Integer Counter	Counter64 0 - 18446744073709551615
media_bytes_received	Total number of media bytes received	Integer Counter	Counter64 0 - 18446744073709551615
media_bytes_sent	Total number of media bytes sent	Integer Counter	Counter64 0 - 18446744073709551615
media_bytes_dropped	Total number of media bytes dropped	Integer Counter	Counter64 0 - 18446744073709551615

Table 25 SmartEdge OS Variables for IPsec Global Schema Profiles

Variable	Description	Type	Value
current_num_of_tunnels	Total number of current tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 25 SmartEdge OS Variables for IPsec Global Schema Profiles

Variable	Description	Type	Value
new_tunnels_up_in_report_interval	Total number of new tunnels established in the reporting interval.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
tunnels_torn_down_in_report_interval	Total number of existing tunnels torn down in the reporting interval.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 26 SmartEdge OS Variables for IPsec Tunnel Schema Profiles

Variable	Description	Type	Value
out_pkts_for_tunnel	Total number of outgoing packets in a tunnel.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_for_tunnel	Total number of incoming packets in a tunnel.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_tunnel_data_in_bytes	Total number of tunneling data, in bytes, for a tunnel.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
out_detunnel_data_in_bytes	Total number of detunneling data, in bytes, for a tunnel.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_trafficselector_mismatch	Total number of discarded incoming packets due to mismatch with the traffic selectors for the child Security Association (SA), through which packets were received.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 26 SmartEdge OS Variables for IPsec Tunnel Schema Profiles

Variable	Description	Type	Value
in_pkts_anti_replay_fail	Total number of discarded incoming packets due to anti-replay check failure.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_integrity_fail	Total number of discarded incoming packets due to integrity check failure.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_decrypt_fail	Total number of discarded incoming packets due to decryption failure.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
out_pkts_seq_no_fail	Total number of discarded outgoing packets due to sequence number overflow.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
out_pkts_child_sa_missing	Total number of discarded outgoing packets due to required child SA failure.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_spi_mismatch	Total number of received IP or ESP packets, with a Security Parameter Index (SPI), which does not match an existing SA.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
out_pkts_for_tunnel_per_qos	Total number of outgoing packets for the tunnel per QoS queue (0-3).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_pkts_for_tunnel_per_qos_q	Total number of incoming packets for the tunnel per QoS queue (0-3).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 26 SmartEdge OS Variables for IPsec Tunnel Schema Profiles

Variable	Description	Type	Value
out_drop_pkts_for_tunnel_per_qos_q	Total number of dropped outgoing packets for the tunnel per QoS queue (0-3).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
in_drop_pkts_for_tunnel_per_qos_q	Total number of dropped incoming packets for the tunnel per QoS queue (0-3).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_frag_pkts_in_tunnel_direction	Total number of fragmented packets received in the tunneling direction.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
frag_pkts_in_tunnel_direction	Total number of packets require fragmentation in the tunneling direction.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_frag_pkts_in_detunnel_direction	Total number of fragmented packets received in the detunneling direction.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 27 SmartEdge OS Variables for IPsec ASP Schema Profiles

Variable	Description	Type	Value
current_num_of_tunnels	Total number of current tunnels (based on last sample)	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
new_tunnels_up_in_report_interval	Total number of new tunnels established in the reporting interval	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
tunnels_torn_down_in_report_interval	Total number of existing tunnels torn down in the reporting interval.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 27 SmartEdge OS Variables for IPsec ASP Schema Profiles

Variable	Description	Type	Value
rcvd_pkts_per_asp_qos_q	Total number of packets received per Octeon QoS Queue (excluding internal queues).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_bytes_per_asp_qos_q	Total number of bytes received per Octeon QoS Queue (excluding internal queues).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
drop_pkts_per_asp_qos_q	Total number of dropped packets per Octeon QoS Queue (excluding internal queues).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
drop_bytes_per_asp_qos_q	Total number of bytes dropped per Octeon QoS Queue (excluding internal queues).	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_pkts_from_lc_for_eco_tunnels	Total number of received packets from each line card slot for economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_bytes_from_lc_for_eco_tunnels	Total number of bytes received from each line card slot for economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
sent_pkts_to_lc_for_eco_tunnels	Total number of packets sent to each line card slot for economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
sent_bytes_to_lc_for_eco_tunnels	Total number of bytes sent to each line card slot for economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
rcvd_pkts_from_lc_for_non_eco_tunnels	Total number of packets received from each line card slot for non-economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 27 SmartEdge OS Variables for IPsec ASP Schema Profiles

Variable	Description	Type	Value
rcvd_bytes_from_lc_for_non_eco_tunnels	Total number of bytes received from each line card slot for non-economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
sent_pkts_to_lc_for_non_eco_tunnels	Total number of packets sent to each line card slot for non-economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
sent_bytes_to_lc_for_non_eco_tunnels	Total number of bytes sent to each line card slot for non-economical tunnels.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
cp_mem_utilization	Control Plane Memory Utilization.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615
cp_cpu_utilization	Control Plane CPU Utilization.	double	Negative Value 1.79769313486231570E+308 through -4.94065645841246544E-324 Positive Value 4.94065645841246544E-324 through 1.79769313486231570E+308
dp_mem_utilization	Data Plane Memory Utilization.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

Table 27 SmartEdge OS Variables for IPsec ASP Schema Profiles

Variable	Description	Type	Value
dp_cpu_utilization_per_core	Data Plane CPU Utilization (per core).	double	Negative Value 1.79769313486231570E+308 through -4.94065645841246544E-324 Positive Value 4.94065645841246544E-324 through 1.79769313486231570E+308
drop_pkts_per_egress_slot	Total number of egress packet drops per egress slot.	uint64_t (Unsigned Integer, 64 bit)	Counter64 0 - 18446744073709551615

1.79.6 Examples

The following example shows how to create a bulkstats schema profile, `prfl-port`, for a port and applies that profile to an Ethernet port using the `bulk` policy:

```
[local]Redback(config)#bulkstats
schema profile port prfl-port format "%d/%d desc: %s" slot port description


[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#bulkstats schema prfl-port policy bulk
```

The following example shows how to create a bulkstats subscriber schema profile that uses the `policing_class_counters` and `metering_class_counters` subscriber schema variables:

```
[local]Redback(config)#
bulkstats schema profile subscriber SubSchema format "session_id: %s,
cct_handle: %s \n Policing Class Counters: %s \n Metering Class Counters: %s" session_id
cct_handle policing_class_counters metering_class_counters
```

1.80 burst-creation-rate

burst-creation-rate ***value***

default burst-creation-rate

1.80.1 Purpose

Establishes the number of flows created, per second, on a circuit.

1.80.2 Command Mode

Flow configuration

1.80.3 Syntax Description

value	Number of flows created on a circuit in one second. The range of values is 1 to 2097152.

1.80.4 Default

None

1.80.5 Usage Guidelines

Use the **burst-creation-rate** command to establish the number of flows created per second.

Use the **default** form of this command to set the creation rate to the previously set value.

1.80.6 Examples

The following example shows how to set the burst creation rate to `2000`:

```
[local]Redback(config-flow-ac-profile)#burst-creation-rate 2000
```

Glossary

MLPPP
Multilink PPP

MP
Multilink PPP

PPA2
Second-generation Packet Processing ASIC

second-generation line card
A PPA2 line card.