# Commands: o through po

COMMAND DESCRIPTION

### Copyright

### Disclaimer

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

### Trademark List

| | |
|---|---|
| **SmartEdge** | is a registered trademark of Telefonaktiebolaget LM Ericsson. |

# Contents

**1 Command Descriptions 1**

1.1 oam fault-monitor 1

1.2 oam manage 3

1.3 oam xc 6

1.4 offer-lease-time 8

1.5 offset-list 10

1.6 oif-interface 12

1.7 on-demand-diagnostic 13

1.8 optimize replication 15

1.9 option 16

1.10 option-82 25

1.11 option domain name-server 27

1.12 option domain-search 28

1.13 option information-refresh-time 29

1.14 option preference 31

1.15 option rapid-commit 33

1.16 optional-checksums 34

1.17 originate-default 35

1.18 originating-rp 37

1.19 originating-rp sa-filter 38

1.20 out-label 39

1.21 output-delay 40

1.22 over-subscription-factor 41

1.23 over-subscription-rate 43

1.24 p2p-port 45

1.25 paired-mode 46

1.26 packet-interval 50

1.27 parameter 52

1.28 parent-class 55

1.29 partition 57

1.30 passive 59

1.31 passive-interface 61

1.32 password 63
1.33 password (BGP) 64
1.34 path-trace 65
1.35 path-trace (ATM OC, POS, WAN-PHY) 67
1.36 pe-type 69
1.37 peer-as 71
1.38 peer-end-point 72
1.39 peer-group 74
1.40 peer id 77
1.41 peer ip-address 78
1.42 peer (L2TP) 79
1.43 peer (L2VPN profile) 81
1.44 peer (MSDP) 82
1.45 peer (NTP) 83
1.46 periodic 84
1.47 permit (IPv4 ACL) 86
1.48 permit (IPv6 ACL) 99
1.49 {permit I deny} 108
1.50 pim accept-rp 113
1.51 pim anycast-rp 114
1.52 pim bfd 115
1.53 pim bsr-border 116
1.54 pim bsr-candidate 118
1.55 pim dense-mode 119
1.56 pim dr-priority 120
1.57 pim dual-join 121
1.58 pim graceful-restart 122
1.59 pim hello-interval 124
1.60 pim neighbor-filter 125
1.61 pim operation-mode 126
1.62 pim rp-address 128
1.63 pim rp-candidate 130
1.64 pim sparse-mode 131
1.65 pim spt-threshold infinity 133
1.66 pim ssm 135
1.67 pim state-refresh origination-interval 137

1.68 pim static group 139
1.69 ping 141
1.70 ping ancp 145
1.71 ping arp 147
1.72 ping atm 149
1.73 ping cpe 151
1.74 ping ipv6 153
1.75 ping mpls ldp 156
1.76 ping mpls mac-address 159
1.77 ping mpls pw 166
1.78 ping mpls rsvp 172
1.79 policy access-list 174
1.80 policy-refresh 180
1.81 pool 221
1.82 port atm 222
1.83 port bvi 224
1.84 port channelized-oc12 227
1.85 port channelized-oc3 227
1.86 port channelized-stm1 227
1.87 port channelized-stm4 227
1.88 port ds0s 227
1.89 port {ds1 | channelized-ds1} 230
1.90 port {ds3 | channelized-ds3} 233
1.91 port {e1 | channelized-e1} 236
1.92 port ethernet 239
1.93 port (http) 242
1.94 port-limit 243
1.95 port <port-type> 245
1.96 port pos 248
1.97 port-priority 250
1.98 port-propagate qos from ethernet 251
1.99 port-propagate qos from ip 253
1.100 port-propagate qos from mpls 256
1.101 port pseudowire 258
1.102 port (RFlow) 259

# 1 Command Descriptions

Commands starting with “o” through commands starting with “po” 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 oam fault-monitor

```
oam fault-monitor end-to-end
```

```
{no | default} oam fault-monitor
```

### 1.1.1 Purpose

Enables alarm indication signal (AIS) and remote defect indication (RDI) fault monitoring for any Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) that references this profile and is not cross-connected.

### 1.1.2 Command Mode

- ATM profile configuration

### 1.1.3 Syntax Description

| | |
|---|---|
| `end-to-end` | Specifies that the fault monitoring is end to end. |

### 1.1.4 Default

Fault monitoring is disabled.

### 1.1.5 Usage Guidelines

Use the **`oam fault-monitor`** command to enable AIS and RDI fault monitoring of any ATM PVC that references this profile.

In compliance with the ITU standard, AIS is used to report faults in the upstream (forward) direction; RDI is used to report faults in the downstream (backward) direction.

If you reference this profile when configuring an ATM PVC that is later cross-connected, this command is disabled (ignored) in the profile.

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

Use the **`no`** or **`default`** form of this command to disable fault monitoring.

### 1.1.6 Examples

The following example shows how to enable fault monitoring for an ATM profile, **oam:**

```
[local]Redback(config)#atm profile oam
[local]Redback(config-atm-profile)#oam fault-monitor end-to-end
```

## 1.2 oam manage

**oam manage end-to-end** [**heartbeat** [**backwards**] | **auto-loopback** [**down-retry-count** ***retries***] [**regular-timeout** ***interval***] [**retry-timeout** ***interval***] [**up-retry-count** ***retries***]]

**no oam manage** [**end-to-end** [**heartbeat** [**backwards**] | **auto-loopback** [**down-retry-count** ***retries***] [**regular-timeout** ***interval***] [**retry-timeout** ***interval***] [**up-retry-count** ***retries***]]]

**default oam manage end-to-end** {**heartbeat** | **auto-loopback**}

### 1.2.1 Purpose

Enables the operational state of any Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) that is not cross-connected and that references this profile to be controlled by the state of its remote defect indication (RDI) and alarm indication signal (AIS) state at the F5 level.

### 1.2.2 Command Mode

ATM profile configuration

### 1.2.3 Syntax Description

| | |
|---|---|
| **end-to-end** | Specifies that the operations, administration, and maintenance (OAM) management is end to end. |
| **heartbeat** | Optional. Specifies continuity monitoring. |
| **backwards** | Optional. Specifies downstream continuity monitoring. |
| **auto-loopback** | Optional. Causes the system to detect and clear the RDI and AIS state. |
| **down-retry-count** ***retries*** | Optional. Number of unsuccessful retries before declaring the connection to be Down. The range of values is 0 to 10; the default value is 3 retries. |
| **regular-timeout** ***interval*** | Optional. Loopback interval in seconds when connectivity is stable. The range of values is 1 to 300; the default value is 30 seconds. |

| | |
|---|---|
| `retry-timeout` *`interval`* | Optional. Loopback interval in seconds when connectivity is changing. The range of values is 1 to 30; the default value is 3 seconds. |
| `up-retry-count` *`retries`* | Optional. Number of successful retries before declaring the connection to be up. The range of values is 0 to 10; the default value is 2 retries. |

### 1.2.4 Default

OAM management is disabled.

### 1.2.5 Usage Guidelines

Use the **`oam manage`** command to enable the operational state of any ATM PVC that references this profile to be controlled by the state of its RDI and AIS state at the F5 level. If the F5 RDI and AIS state is active, the operational state of the ATM PVC is down; if F5 RDI and AIS state is not active, the operational state is up.

If you reference this profile when configuring an ATM PVC that is later cross-connected, this command is disabled (ignored) in the profile.

Use the **`heartbeat`** keyword to enable continuity monitoring. Cells are issued repetitively with a periodicity of one cell each second independently of user cell traffic. After enabling continuity monitoring, if the PVC does not receive any monitoring cell within a time interval of 3.5 seconds, with a margin of ±.5 seconds, from a peer that is configured with continuity checking (heartbeat backward), the system declares a VP-AIS or a virtual circuit (VC)-AIS (or both) state due to a loss of continuity.

Use the **`auto-loopback`** keyword to cause the system to detect and clear the RDI/AIS state by using OAM F4 and F5 loopback cells to be periodically transmitted and its response cells monitored when appropriate.

If you specify either the **`heartbeat`** or the **`auto-loopback`** keyword, the operational state is controlled by both RDI/AIS, and either continuity check cells or ATM OAM loopback cells.

If you specify neither the **`heartbeat`** nor the **`auto-loopback`** keyword, OAM management is enabled with only the fault monitoring function.

In every case, the system monitors and reacts to an RDI/AIS state by declaring the ATM PVC down and sending an Simple Network Management Protocol (SNMP) trap.

**Note:** By default, because an ATM PVC is enabled when you create it, OAM management is in effect for any ATM PVC that references a profile that includes the **`oam manage`** command. However, if you disable the ATM PVC with the **`shutdown`** command (in ATM PVC configuration mode), then OAM management is not in effect. You must enable the ATM PVC with the **`no shutdown`** command (in ATM PVC configuration mode) for OAM management to determine the state of the ATM PVC.

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

Use the **`no`** or **`default`** form of this command to disable OAM management of any ATM PVC that references this profile.

To display the values of the auto-loopback parameters and the ATM PVC status, enter the **`show atm pvc`** command (in any mode).

### 1.2.6 Examples

The following example shows how to enable the operational state of any ATM PVC that references the **oam** profile to be controlled by both the state of its RDI/AIS and by OAM loopback:

```
[local]Redback(config)#atm profile oam
[local]Redback(config-atm-profile)#oam manage end-to-end auto-loopback
 regular-timeout 45
```

# 1.3 oam xc

**oam xc end-to-end** {[**loopback**] [**heartbeat**] [**ais/rdi**]}

{**no** | **default**} **oam xc**

## 1.3.1 Purpose

Enables operations, administration, and maintenance (OAM) cells received on one of a pair of cross-connected Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that reference this profile to be forwarded to and transmitted on the other ATM PVC.

## 1.3.2 Command Mode

- ATM profile configuration

## 1.3.3 Syntax Description

| | |
|---|---|
| `end-to-end` | Specifies that the operations, administration, and maintenance (OAM) management is end to end. |
| `loopback` | Optional. Specifies that the OAM loopback cells are to be forwarded. |
| `heartbeat` | Optional. Specifies continuity monitoring; the OAM continuity check cells are forwarded. |
| `ais/rdi` | Optional. Specifies that the OAM alarm indication signal (AIS) and remote defect indication (RDI) fault monitoring cells are to be forwarded. |

## 1.3.4 Default

No OAM cells are forwarded

## 1.3.5 Usage Guidelines

Use the **oam xc** command to enable the OAM cells received on one of a pair of cross-connected ATM PVCs that reference this profile to be forwarded to and transmitted on the other ATM PVC.

If you reference this profile when configuring an ATM PVC that is not cross-connected, this command is disabled (ignored) in the profile; if the profile is also configured with either the **oam fault-monitor** or **oam manage** command (in ATM profile configuration mode), that command is enabled instead. If the ATM PVC is cross-connected at a later time, this command in the profile is enabled and either the **oam fault-monitor** or **oam manage** command is disabled.

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

Use the `no` or `default` form of this command to disable the forwarding of all OAM cells.

### 1.3.6 Examples

The following example selectively disables the heartbeat option:

```
[local]Redback(config)#atm profile oam-xc
[local]Redback(config-atm-profile)#oam xc end-to-end loopback ais/rdi
```

The following example shows how to enable all OAM cells to be forwarded across the cross-connection of two ATM PVCs on ATM OC ports:

```
[local]Redback(config)#atm profile oam-xc
[local]Redback(config-atm-profile)#oam xc end-to-end loopback heartbeat ais/rdi
[local]Redback(config-atm-profile)#exit
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-oc)#atm pvc 100 100 profile oam-xc encapsulation raw
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#atm pvc 100 100 profile oam-xc encapsulation raw
[local]Redback(config-atm-oc)#exit
[local]Redback(config)#xc 3/1 vpi-vci 100 100 to 4/1 vpi-vci 100 100
```

## 1.4 offer-lease-time

```
offer-lease-time seconds

no offer-lease-time seconds
```

### 1.4.1 Purpose

Specifies the offer lease time for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

### 1.4.2 Command Mode

- DHCP server configuration
- DHCP subnet configuration

### 1.4.3 Syntax Description

| | |
|---|---|
| *seconds* | Length of time for the default lease. The range of values is 60 (one minute) to 360 (one l |

### 1.4.4 Default

The default value for the offer lease time is two minutes.

### 1.4.5 Usage Guidelines

Use the `offer-lease-time` command to specify the offer lease time for the DHCP server or one of its subnets. When entered in DHCP server configuration mode, specifies the offer lease time for the server and all its subnets; when entered in DHCP subnet configuration mode, specifies offer lease time for that subnet. The value specified for a subnet overrides the global value for the server.

Use the `no` form of this command to specify the default value for the offer lease time.

### 1.4.6 Examples

The following example specifies an offer lease time of 5 minutes (**300**) for the DHCP server and all its subnets:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#offer-lease-time 300
```

# 1.5 offset-list

**`offset-list`** ***`pl-name`*** {**`in`** | **`out`**} ***`offset`***

**`no offset-list`** ***`pl-name`*** {**`in`** | **`out`**} ***`offset`***

## 1.5.1 Purpose

Configure a Routing Information Protocol (RIP) offset list.

## 1.5.2 Command Mode

RIP router configuration

## 1.5.3 Syntax Description

| | |
|---|---|
| ***`pl-name`*** | IP prefix list name. |
| **`in`** | Adds offset to incoming RIP updates. |
| **`out`** | Adds offset to outgoing RIP updates. |
| ***`offset`*** | Offset value. The range of values is 1 to 16. |

## 1.5.4 Default

No RIP offset list is configured.

## 1.5.5 Usage Guidelines

Use the **`offset-list`** command to configure a RIP offset list. A RIP offset list adds to the cost metric of inbound or outbound routes learned or advertised by RIP. RIP offset lists provide a method for adding to the cost metric of routes, which moves the routing switch’s route selection away from those routes.

The RIP offset list adds the offset value to the cost metric of all routes that match the specified prefix list.

Use the **`no`** form of this command to remove the RIP offset list.

### 1.5.6 Examples

The following example configures a RIP offset list to add **8** to the cost metric for all routes that match the IP prefix list, **foo23:**

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#offset-list foo23 in 8
```

# 1.6 oif-interface

**`oif-interface`** *`interface`*

**`no oif-interface`**

## 1.6.1 Purpose

Identifies an interface connected to the subscriber device in a PIM-Dual Join implementation.

## 1.6.2 Command Mode

pim-dual configuration mode

## 1.6.3 Syntax Description

| | |
|---|---|
| *`interface`* | Interface connected to the subscriber device. |

## 1.6.4 Default

None

## 1.6.5 Usage Guidelines

Use the **`oif-interface`** command to identify an interface connected to the subscriber device in a PIM-Dual Join implementation.

Use the **`no`** form of this command to identify the interface previously set.

## 1.6.6 Examples

The following example shows how to identify the interface **int1** as the interface connected to the subscriber device in a PIM-Dual Join implementation:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#pim dual-join group 225.100.1.1 source 192.110.30.6
[local]Redback(config-pim-dual)#oif-interface int1
```

# 1.7 on-demand-diagnostic

```
on-demand-diagnostic
```

```
no on-demand-diagnostic
```

## 1.7.1 Purpose

Places an I/O carrier card, services card, or line card in the on-demand diagnostics (ODD) state.

## 1.7.2 Command Mode

- card configuration

## 1.7.3 Syntax Description

This command has no keywords or arguments.

## 1.7.4 Default

None

## 1.7.5 Usage Guidelines

Use the `on-demand-diagnostic` command to place a carrier, line, or services card in the ODD state.

This command is available only for the SmartEdge 100 I/O carrier card in slot 2 and the following SmartEdge line cards:

- ATM OC-12c/STM-3c, and second-generation ATM OC line cards
- Fast Ethernet-Gigabit Ethernet line cards
- Gigabit Ethernet line cards (any version)
- SONET/SDH OC-3c/STM-1c, OC-12c/STM-4c, OC-48c/STM-16c, and OC-192c/STM-64c line cards

**Note:** The correspondence between the card name that appears in the CLI and the line card type is found in *Card Types* section of the `Configuring Cards` document.

Low-density versions of these line cards are also supported, but only the enabled ports are tested.

You must place the carrier card or line card in the out-of-service state with the **shutdown** command in ATM OC port configuration mode before you can enter this command. Specify slot 2 when you shut down the carrier card to shut down the I/O functions.

Use the **no** form of this command to remove the carrier card or line card from the ODD state.

### 1.7.6 Examples

The following example places the I/O carrier card (slot **2**) in the ODD state:

```
[local]Redback(config)#card carrier 2
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#end
```

The following example places the Ethernet line card in slot 3 in the ODD state:

```
[local]Redback(config)#card 10ge-1-port 3
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#end
```

# 1.8 optimize replication

```
optimize replication

no optimize replication
```

## 1.8.1 Purpose and Usage Guidelines

Enables packet mesh ASIC (PMA)-based traffic replication on the current line card to the destination line cards. When not enabled, packet replication is performed in the ingress packet processing ASICs (PPAs).

Use the `optimize replication` command to support high-bandwidth multicast services such as IPTV.

- This command is only supported on PPA3-based line cards: Gigabit Ethernet 20-port card (ge4-20-port) and 10 Gigabit Ethernet 4-port card (10ge-4-port).

- Mesh-based traffic replication is performed only on traffic sent to PPA3 destination line cards. This command has no effect on multicast traffic sent to PPA2 destination cards.

- All multicast traffic to destination PPA3 cards, belonging to any service (for example, IP routing, Layer-2 bridging), is replicated using the packet mesh.

- A maximum of two line cards in a system can be set to optimize replication. For example, you could assign two uplink (or trunk) ports carrying IPTV traffic for distribution among downlink ports.

- On the packet mesh, the queue and backplane priority of optimized multicast traffic is fixed at priority 1, which is just above the Differentiated Services Code Point (DSCP) value of unicast AF4 class (CS4) (IP precedence 4 FlashOver).

- Enabling or disabling this command causes traffic interruption of less than 1 second on the card.

## 1.8.2 Command Mode

card configuration

## 1.8.3 Syntax Description

This command has no arguments.

### 1.8.4 Default

Packet replication is performed on the ingress PPA. Use the **no** form of this command to return the card to the default condition.

### 1.8.5 Examples

```
[local]Redback#card 10ge-4-port
[local]Redback(config-card)#optimize replication
```

## 1.9 option

**option** {*opt-num* | *opt-name*} *opt-arg1* [*opt-arg2* [*opt-arg3* [*opt-arg4*]]]

**no option** {*opt-num* | *opt-name*}

### 1.9.1 Purpose

Specifies an option for this internal Dynamic Host Configuration Protocol (DHCP) server or one of its subnets.

### 1.9.2 Command Mode

- DHCP server configuration
- DHCP subnet configuration

### 1.9.3 Syntax Description

| | |
|---|---|
| *opt-num* | DHCP option number; the range of values is 1 to 125. Table 1 to Table 7 list the option numbers. |
| *opt-name* | DHCP option name. Table 1 to Table 7 list the option names. |
| *opt-arg1* | First argument for the DHCP option. Table 1 to Table 7 list the arguments for the DHCP options. |
| *opt-arg2* ... *opt-arg4* | Optional. Additional values for a DHCP option with an IP address argument. If *opt-arg1* is an IP address, you can specify up to three additional IP addresses. |

### 1.9.4 Default

No DHCP options are specified for the DHCP server or for any of its subnets.

### 1.9.5 Usage Guidelines

Use the `option` command to specify an option for this internal DHCP server or for one of its subnets. When you enter this command in DHCP server configuration mode, it specifies the DHCP option for the server and all its subnets; when you enter it in DHCP subnet configuration mode, it specifies the option for that subnet. The value specified for a subnet overrides the global value for the server.

You can enter this command multiple times to specify as many different DHCP options as you require. Succeeding entries for the same DHCP option overwrite any previously entered value.

You can specify up to four IP addresses for a DHCP option that requires an IP address. If the DHCP option also requires an netmask argument in addition to the IP address, you can specify up to two IP addresses and their netmask arguments.

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, Section 3 through Section 9 describe the option numbers, names, and arguments. Table 1 to Table 7 list this data for the options in each section; options are listed by code within each table.

Use the `no` form of this command to remove the option from the internal DHCP server or subnet configuration.

**Note:** DHCP can send RADIUS-specified vendor-encapsulated options to the DHCP client. RADIUS sends the vendor-encapsulated options using the vendor-specific attribute (VSA) 127 (DHCP-Vendor-Encap-Options) provided by Ericsson AB. For more information about the format for VSA 127, see *Redback VSAs Supported by the SmartEdge Router* in *RADIUS Attributes*.

*Table 1 RFC 1497 Vendor Extensions*

| Option Code Name | Argument | Argument Description | Option Description | |
|---|---|---|---|---|
| 1 | **`subnet-mask`** | *`netmask`* | Netmask in the format ***`E.F.G.H`***. | Configure the subnet mask supplied to the client. |
| 2 | **`time-offset`** | *`seconds`* | Signed integer; the range of values is –2,147,483,648 to +2,147,483,648. | Configure the time offset value. |
| 3 | **`router`** | *`ip-addr`* | IP address in the format ***`A.B.C.D`***. | Configure the router that the client can use. |
| 4 | **`time-server`** | *`ip-addr`* | IP address in the format ***`A.B.C.D`***. | Configure the time server. |

*Table 1 RFC 1497 Vendor Extensions*

| Option Code Name | Argument | Argument Description | Option Description | |
|---|---|---|---|---|
| 5 | `ien116-name-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the IEN116 name server. |
| 6 | `domain-name-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the domain name server. |
| 7 | `log-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the log server. |
| 8 | `cookie-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the cookie server. |
| 9 | `lpr-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the line printer (LPR) server. |
| 10 | `impress-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the impress server. |
| 11 | `resource-location-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the resource location server. |
| 12 | `host-name` | *name* | Name of the host. | Configure the hostname, which can include its domain name. |
| 13 | `boot-size` | *size* | File size in 512-octet blocks; the range of values is 0 to 65,535. | Configure the size of the boot file. |
| 14 | `merit-dump` | *path* | Path, including the filename. | Configure the path to the merit dump file. |
| 15 | `domain-name` | *dom-name* | Domain name; must be “redback.com” (without quotes). | Configure the domain name. |
| 16 | `swap-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the swap server. |
| 17 | `root-path` | *path* | Path to the root disk. | Configure the path to the root disk. |
| 18 | `extensions-path` | *path* | Path to the extensions. | Configure the extensions path. |

*Table 2 IP Layer Parameters for a Host*

| Option Num Name | Argument | Argument Description | Option Description | |
|---|---|---|---|---|
| 19 | `ip-forwarding` | *boolean-flag* | • `0`—Disables IP layer for forwarding.<br>• `1`—Enables IP layer for forwarding. | Configure IP forwarding. |
| 20 | `non-local-source-routing` | *boolean-flag* | • `0`—Disables forwarding of datagrams with nonlocal source routes.<br>• `1`—Enables forwarding of datagrams with nonlocal source routes. | Configure non-local source routing. |
| 21 | `policy-filter` | *ip-addr*<br>*netmask* | IP address in the format ***A.B.C.D***.<br>Netmask in the format ***E.F.G.H***. | Configure a policy filter. |
| 22 | `max-dgram-reassembly` | *max-size* | Maximum size of any datagram that needs reassembly; the range of values is 0 to 65,535. | Configure the maximum size for datagram reassembly. |
| 23 | `default-ip-ttl` | *seconds* | The range of values is 0 to 255. | Configure the default IP time-to-live value. |
| 24 | `path-mtu-aging-timeout` | *seconds* | The range of values is 0 to 4,294,967,295. | Configure the timeout value to use when aging path maximum transmission units (MTUs). |
| 25 | `path-mtu-plateau-table` | *mtu* | The range of values is 0 to 65,535. | Configure the table of MTU sizes for use when performing Path MTU discovery. |

*Table 3 IP Layer Parameters for an Interface*

| Option Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 26 | `interface-mtu` | *mtu* | The range of values is 0 to 65,535. | Configure the interface MTU. |
| 27 | `all-subnets-local` | *boolean-flag* | • `0`—Some subnets can have smaller MTUs.<br>• `1`—All subnets share the same MTU. | Configure all subnets are local. |
| 28 | `broadcast-address` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the broadcast IP address. |
| 29 | `perform-mask-discovery` | *boolean-flag* | • `0`—Client does not perform mask discovery.<br>• `1`—Client performs mask discovery. | Configure mask discovery. |
| 30 | `mask-supplier` | *boolean-flag* | • `0`—Client should not respond.<br>• `1`—Client should respond. | Configure the mask supplier. |
| 31 | `router-discovery` | *boolean-flag* | • `0`—Client should perform router discovery.<br>• `1`—Client should not perform router discovery. | Configure router discovery. |
| 32 | `router-solicitation -address` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the router solicitation IP address. |
| 33 | `static-route` | *ip-addr*<br>*netmask* | • IP address in the format ***A.B.C.D***.<br>• Netmask in the format ***E.F.G.H***. | Configure the static route. |

*Table 4 Link Layer Parameters for an Interface*

| Option Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 34 | `trailer-encapsulation` | *boolean-flag* | • `0`—Client should not attempt to use trailers.<br>• `1`—Client should attempt to use trailers. | Configure trailer encapsulation. |
| 35 | `arp-cache-timeout` | *seconds* | The range of values is 0 to 4,294,967,295. | Configure the Address Resolution Protocol (ARP) cache timeout. |
| 36 | `ieee802-3-encapsulation` | *boolean-flag* | • `0`—Client should use Ethernet version 2 encapsulation (RFC 894[1]).<br>• `1`—Client should use Ethernet IEEE 802.3 encapsulation (RFC 1042[2]). | Specify Ethernet encapsulation. |

*[1] RFC 894, Standard for the Transmission of IP Datagrams over Ethernet Networks*
*[2] RFC 1042, Standard for the Transmission of IP Datagrams over IEEE 802 Ethernet Networks*

*Table 5 TCP Parameters*

| Option Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 37 | `default-tcp-ttl` | *seconds* | The range of values is 0 to 255. | Configure the default Transmission Control Protocol (TCP) time-to-live value. |
| 38 | `tcp-keepalive-interval` | *seconds* | The range of values is 0 to 4,294,967,295. | Configure the TCP keepalive interval. |
| 39 | `tcp-keepalive-garbage` | *boolean-flag* | • `0`—Client should not send garbage octet.<br>• `1`—Client should send garbage octet. | Configure the use of a TCP keepalive garbage octet. |

*Table 6 Application and Service Parameters*

| Optio n Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 40 | `nis-domain` | *dom-name* | NIS domain. | Configure the Network Information Server (NIS) domain. |
| 41 | `nis-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the NIS server. |
| 42 | `ntp-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the Network Time Protocol (NTP) server. |
| 43 | `vendor-encapsulated -options` | Can be:<br>• **numeric** *num*<br>• **string** *name* | • *num*—Option number.<br>• *name*—Option name. | Configure a vendor-encapsulated option. |
| 44 | `netbios-name-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the NetBIOS name server. |
| 45 | `netbios-dd-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the NetBIOS datagram distribution (DD) server. |
| 46 | `netbios-node-type` | *type* | The range of values is 0 to 255. | Configure the NetBIOS node type. |
| 47 | `netbios-scope` | *scope* | NetBIOS scope parameter. | Configure the NetBIOS scope parameter, as specified in RFCs 1001(1) and 1002(2). |
| 48 | `font-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the font server. |
| 49 | `x-display-manager` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the X window system display manager. |
| 64 | `nisplus-domain` | *dom-name* | NIS+ domain. | Configure the NIS+ domain. |
| 65 | `nisplus-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the NIS+ server. |
| 68 | `mobile-ip-home-agent` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the mobile IP home agent. |
| 69 | `smtp-server` | *ip-addr* | IP address in the format ***A.B.C.D***. | Configure the Simple Mail Transport Protocol (SMTP) server. |

Table 6 Application and Service Parameters

| Option Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 70 | `pop-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the Post Office Protocol (POP3) server. |
| 71 | `nntp-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the Network News Transport Protocol (NNTP) server. |
| 72 | `www-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the WWW server. |
| 73 | `finger-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the finger server. |
| 74 | `irc-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the default Internet Relay Chat (IRC) server. |
| 75 | `streettalk-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the StreetTalk server. |
| 76 | `streettalk-directory -assistance-server` | *ip-addr* | IP address in the format *A.B.C.D*. | Configure the StreetTalk directory assistance (STDA) server. |

*(1) RFC 1001, Protocol Standard for a NetBIOS Service on a TCP/UDP transport: Concepts and Methods*

*(2) RFC 1002, Protocol Standard for a NetBIOS Service on a TCP/UDP transport: Detailed Specifications*

Table 7 DHCP Extension Parameters

| Option Num Name | Argument | Argument Description | Description | |
|---|---|---|---|---|
| 66 | `tftp-server-name` | *name* | TFTP server name. | Configure the Trivial File Transfer Protocol (TFTP) server. |
| 67 | `bootfile-name` | *name* | Boot filename. | Configure the name of the boot loader image file. |

### 1.9.6 Examples

The following example specifies the options for an internal DHCP server (and its subnets), which are overridden by the options for the **sub2** subnet:

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

! Specify global options (these apply to all subnets)

[local]Redback(config-dhcp-server)#option domain-name redback.com
[local]Redback(config-dhcp-server)#option domain-name-server 10.1.1.254

! Create a subnet; specify options for this subnet, which override the global settings

[local]Redback(config-dhcp-server)#subnet 10.1.1.1/24 name sub2
[local]Redback(config-dhcp-subnet)#option router 10.1.1.1
[local]Redback(config-dhcp-subnet)#option domain-name hot.com
```

The following example adds a second IP address for the **router** option in the **sub2** subnet configuration and includes option **21** (policy-filter) with two IP addresses and their netmasks:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 10.1.1.1/24 name sub2
[local]Redback(config-dhcp-subnet)#option router 10.1.1.1 10.1.1.2

[local]Redback(config-dhcp-subnet)#option 21 10.1.1.23 255.255.255.255
10.1.1.33 255.255.255.255
```

## 1.10 option-82

To specify the circuit agent ID, the syntax is:

```
option-82 circuit-id string [offset position] {ip-address ip-addr
| max-addresses num-addr}
```

```
no option-82 circuit-id string [offset position] {ip-address
ip-addr | max-addresses num-addr}
```

To specify the remote agent ID, the syntax is:

```
option-82 remote-id string [offset position] ip-address ip-addr
```

```
no option-82 remote-id string
```

### 1.10.1 Purpose

Creates a static mapping between the Agent-Circuit-Id subfield or the Agent-Remote-Id subfield in the option 82 field and an IP address.

### 1.10.2 Command Mode

- DHCP subnet configuration

### 1.10.3 Syntax Description

| | |
|---|---|
| `circuit-id` *`string`* | Circuit agent ID. A text string, with up to 255 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces. |
| `remote-id` *`string`* | Remote agent ID. A text string, with up to 255 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces. |
| `offset` *`position`* | Optional. Position of the starting octet in the option 82 subfield which is to be matched with the specified *`string`* argument, according to one of the following formats:<br>• +n or n—Starting octet is the nth octet in the received Id. The matching operation is performed on the nth and succeeding octets for the length of the string specified by the value of the *`string`* argument.<br>• –n—Starting octet is the last octet in the received Id minus the previous (n–1) octets. The matching operation is performed on the succeeding octets for the length of the string specified by the value of the *`string`* argument.<br>The default value is 1 (the first octet). You can also specify the first octet with a value of 0. |
| `ip-address` *`ip-addr`* | IP address to which the option 82 subfield is to be mapped. |
| `max-addresses` *`num-addr`* | Maximum number of IP addresses permitted for the specified circuit agent ID. |

### 1.10.4 Default

No static mapping is created between an option 82 subfield and any IP address.

### 1.10.5 Usage Guidelines

Use the **option-82** command to create a static mapping between the Agent-Circuit-Id subfield or the Agent-Remote-Id subfield in the option 82 field and an IP address. The option 82 field is sent in the DHCP discover packet.

The value for the ***ip-addr*** argument must be an IP address within this subnet, but not within any range of IP addresses that you have specified using the **range** command (in DHCP subnet configuration mode).

You can specify the remote agent ID and the circuit agent ID in vendor-specific attributes (VSAs) 96 and 97, respectively, using the **radius attribute calling-station-id** and **radius attribute nas-port-id** commands (in context configuration mode). vendor VSAs provided by Ericsson AB are described in *RADIUS Attributes*.

Use the **no** form of this command to delete the static mapping.

### 1.10.6 Examples

The following example creates a static mapping between option 82 Agent-Circuit-Id subfield, **4:1 vlan 102,** and the **12.1.1.11** IP address:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#dhcp server policy
[local]Redback(config-dhcp-server)#subnet 12.1.1.0/24 name sub2
[local]Redback(config-dhcp-subnet)#range 12.1.1.50 12.1.1.100
[local]Redback(config-dhcp-subnet)#mac-address 02:12:34:56:78:90 ip-address 12.1.1.10
[local]Redback(config-dhcp-subnet)#option-82 circuit-id “4:1 vlan 102” offset 3 ip-address 12.1.1.11
```

# 1.11 option domain name-server

**option domain-name-server** ***server-address***

**no option domain-name-server**

## 1.11.1 Purpose

In a DHCPv6 server policy, specifies the IP address of the DNS name server to be used by clients for DNS hostname resolution.

## 1.11.2 Command Mode

DHCPv6 server policy configuration

DHCPv6 server policy subnet configuration

## 1.11.3 Syntax Description

| | |
|---|---|
| *server-address* | Configures an IPv6 address for the DNS name server. |

## 1.11.4 Default

No DNS name server is specified in the DHCPv6 profile.

## 1.11.5 Usage Guidelines

Use the **option domain-name-server** command to specify the IPv6 address of the DNS name server to be used by IPv6 clients for DNS hostname resolution.

Use the **no** version of this command to remove a DNS name server from a DHCPv6 profile.

## 1.11.6 Examples

The following example configures a DHCPv6 server policy to direct clients to use the DNS name server on the IPv6 address 2005:db8:b:3f::2 for DNS hostname resolution:

```
[local]BRAS(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#option domain-name-server 2005:db8:b:3f::2
```

# 1.12 option domain-search

**option domain-search *domain-name***

**no option domain-search**

## 1.12.1 Purpose

In a DHCPv6 server policy, specifies the domain name that a host appends to a hostname for DNS hostname resolution.

## 1.12.2 Command Mode

DHCPv6 server policy configuration

DHCPv6 server policy subnet configuration

## 1.12.3 Syntax Description

| | |
|---|---|
| *domain-name* | Specifies a domain name to be appended to a hostname for DNS resolution. |

## 1.12.4 Default

No DNS name server is specified in the DHCPv6 server policy.

## 1.12.5 Usage Guidelines

Use the **option domain-search** command to specify the domain name that a host appends to a hostname for DNS hostname resolution.

Use the **no** version of this command to remove a specified domain name from a DHCPv6 server policy.

## 1.12.6 Examples

The following example configures the domain search option in a DHCPv6 server policy. In this example, the domain name **SJ1.com** is appended to hostnames queried for DNS resolution:

```
[local]BRAS(config-ctx)#dhcpv6 server

[local]Redback(config-dhcpv6-server)#option domain-search SJ1.com
```

# 1.13 option information-refresh-time

**`option information-refresh-time`** ***`seconds`***

**`no option information-refresh-time`**

## 1.13.1 Purpose

In a DHCPv6 server policy, configures the number of seconds a client waits before refreshing the configuration information received from DHCPv6 server.

## 1.13.2 Command Mode

DHCPv6 server policy configuration

## 1.13.3 Syntax Description

| | |
|---|---|
| *`seconds`* | Number of seconds a client waits before refreshing the configuration information received from DHCPv6 server. Range is from 600 through 4294967295 seconds. |

## 1.13.4 Default

The number of seconds a client waits before refreshing the configuration information received from DHCPv6 server is not specified.

## 1.13.5 Usage Guidelines

Use the **`option information-refresh-time`** command to configure the number of seconds a client waits before refreshing the configuration information received from DHCPv6 server.

Use the **`no`** version of this command to return the DHCPv6 server policy refresh time attribute to the default configuration, where the number of seconds a client waits before refreshing the configuration information received from DHCPv6 server is not specified.

## 1.13.6 Examples

The following example configures the refresh time attribute in a DHCPv6 server policy to be 3000000 seconds. This means clients of this server refresh the configuration information received from this server every 3000000 seconds:

```
[local]Redback(config-ctx)#dhcpv6 server
[local]Redback(config-dhcpv6-server)#option information-refresh-time 3000000
```

## 1.14 option preference

```
option preference integer

no option preference
```

### 1.14.1 Purpose

In a DHCPv6 server policy, configures the preference value for a DHCPv6 server.

### 1.14.2 Command Mode

DHCPv6 server policy configuration

### 1.14.3 Syntax Description

| | |
|---|---|
| *integer* | Preference value for a DHCPv6 server. Servers with a lower value take precedence over servers configured with a higher value. Range is from 0 through 255. |

### 1.14.4 Default

The preference value for a DHCPv6 server is not specified.

### 1.14.5 Usage Guidelines

Use the `option preference` command to configure the preference value for a DHCPv6 server.

A DHCPv6 server configured with a lower value is preferred over a server configured with a higher value.

When a client requests an IPv6 prefix, that client typically accepts the first IPv6 prefix it receives. However, you can configure a DHCPv6 server to be preferred so that the client accepts IPv6 prefixes from that server over any other DHCPv6 server.

Use the `no` version of this command to return the DHCPv6 server preference attribute to the default value.

### 1.14.6 Examples

The following example configures the preference attribute for a DHCPv6 server to be 5:

```
[local]Redback(config-ctx)#dhcpv6 server

[local]Redback(config-dhcpv6-server)#option preference 5
```

# 1.15 option rapid-commit

**option rapid-commit**

**no option rapid-commit**

## 1.15.1 Purpose

Enables RAPID COMMIT in a DHCPv6 server policy (for faster IPv6 prefix delegation).

## 1.15.2 Command Mode

DHCPv6 server policy configuration

## 1.15.3 Syntax Description

This command has no keywords or arguments.

## 1.15.4 Default

RAPID COMMIT is disabled.

## 1.15.5 Usage Guidelines

Use the **option rapid-commit** command to enable RAPID COMMIT in a DHCPv6 server policy (for faster IPv6 prefix delegation).

**Note:** With the RAPID COMMIT option, only two messages (SOLICIT and REPLY messages) are exchanged between the DHCPv6 server and the CPE. The RAPID COMMIT option is typically used when there is only one server for a CPE to connect to.

Use the **no** version of this command to disable RAPID COMMIT in a DHCPv6 server policy.

## 1.15.6 Examples

The following example enables RAPID COMMIT in a DHCPv6 server policy:

```
[local]Redback(config-ctx)#dhcpv6 server

[local]Redback(config-dhcpv6-server)#option rapid-commit
```

# 1.16 optional-checksums

**optional-checksums** [**level-1** | **level-2**]

**no optional-checksums** [**level-1** | **level-2**]

## 1.16.1 Purpose

Enables optional Intermediate System-to-Intermediate System (IS-IS) checksums on the interface.

## 1.16.2 Command Mode

IS-IS interface configuration

## 1.16.3 Syntax Description

| | |
|---|---|
| `level-1` | Optional. Enables checksums for IS-IS level 1 routing independently. |
| `level-2` | Optional. Enables checksums for IS-IS level 2 routing independently. |

## 1.16.4 Default

The command is disabled.

## 1.16.5 Usage Guidelines

Use the **optional-checksums** command to enable optional IS-IS checksums on the interface.

Use the **no** form of this command to disable optional IS-IS checksums.

## 1.16.6 Examples

The following example enables optional checksums on the **fa4/1** interface:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if))#optional-checksums
```

# 1.17 originate-default

**`originate-default`** {**`always`** | **`route-map`** ***`map-name`***} [**`metric`** ***`metric`***] [**`metric-type`** ***`type`***]

**`no originate-default`**

## 1.17.1 Purpose

Originates the default route advertisement in the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) routing domain.

## 1.17.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

## 1.17.3 Syntax Description

| | |
|---|---|
| **`always`** | Always originates a default route. |
| **`route-map`** ***`map-name`*** | Route map name. Originates the default route when all conditions in the specified route map are met and when the route exists in the Route Information Base (RIB). |
| **`metric`** ***`metric`*** | Optional. Metric value for the default route. The range of values is 1 to 16,777,214; the default value is 1. |
| **`metric-type`** ***`type`*** | Optional. External route metric type for a Type 5 default link-state advertisement (LSA). The ***`type`*** argument specifies one of the following metric types:<br>• `1`—Specifies a Type 1 metric type.<br>• `2`—Specifies a Type 2 metric type. |

## 1.17.4 Default

No default route is originated. When this command is used to originate a default route, the metric value is 1.

## 1.17.5 Usage Guidelines

Use the **`originate-default`** command to originate the default route advertisement in the OSPF or OSPFv3 routing domain.

Use the **`no`** form of this command to remove the default route.

### 1.17.6 Examples

The following example configures the OSPF instance to originate a default route when there is a route in the RIB for routes matching the **rmap01** route map:

```
[local]Redback(config-ospf)#originate-default route-map rmap01
```

## 1.18 originating-rp

**`originating-rp`** ***`if-name`***

**`no originating-rp`** ***`if-name`***

### 1.18.1 Purpose

Configures an interface as the originating rendezvous point (RP) address.

### 1.18.2 Command Mode

MSDP router configuration

### 1.18.3 Syntax Description

| | |
|---|---|
| *`if-name`* | Name of the interface whose IP address is to be used as the originating RP address. |

### 1.18.4 Default

None

### 1.18.5 Usage Guidelines

Use the **`originating-rp`** command to configure an interface as the originating RP address. The IP address of the interface is used as the RP address in all source active (SA) messages originated by the router.

Use the **`no`** form of this command to remove the interface's IP address for the originating RP address.

### 1.18.6 Examples

The following example configures the interface, **ToLan04**, to be used as the RP address:

```
[local]Redback(config-msdp)#originating-rp ToLan04
```

# 1.19 originating-rp sa-filter

**originating-rp sa-filter** ***acl-name***

**no originating-rp sa-filter** ***acl-name***

## 1.19.1 Purpose

Configures an access control list (ACL) to filter incoming source active (SA) messages learned from the local rendezvous point (RP).

## 1.19.2 Command Mode

MSDP router configuration

## 1.19.3 Syntax Description

| | |
|---|---|
| *acl-name* | Name of the ACL used to filter incoming SA messages. |

## 1.19.4 Default

None

## 1.19.5 Usage Guidelines

Use the **originating-rp sa-filter** command to configure an ACL to filter incoming SA messages learned from the local RP.

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

## 1.19.6 Examples

The following example configures ACL **320** to filter incoming SA messages:

```
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#originating-rp sa-filter 320
```

# 1.20 out-label

**out-label** ***out-label-num***

## 1.20.1 Purpose

Configures the outgoing label number for a static label-switched path (LSP).

## 1.20.2 Command Mode

MPLS static LSP configuration

## 1.20.3 Syntax Description

| | |
|---|---|
| ***out-label-num*** | Number of the outgoing label. The range of values is 16 to 1,024. |

## 1.20.4 Default

None

## 1.20.5 Usage Guidelines

Use the **out-label** command to configure the outgoing label number for a static LSP.

## 1.20.6 Examples

The following example configures the outgoing label for the LSP, **test14**, to the value of **20:**

```
[local]Redback(config-ctx)#router mpls-static
[local]Redback(config-mpls-static)#lsp test14
[local]Redback(config-mpls-static-lsp)#out-label 20
```

# 1.21 output-delay

**`output-delay`** ***`delay`***

{**`no`** | **`default`**} **`output-delay`**

## 1.21.1 Purpose

Adds a delay time between packets sent in multipacket Routing Information Protocol (RIP) or RIP next generation (RIPng) updates.

## 1.21.2 Command Mode

- RIPng router configuration
- RIP router configuration

## 1.21.3 Syntax Description

| | |
|---|---|
| ***`delay`*** | Amount of delay, in milliseconds, added between packets. The range is of values is 1 to |

## 1.21.4 Default

Packets are sent without a delay.

## 1.21.5 Usage Guidelines

Use the **`output-delay`** command to add a delay time between packets in multipacket RIP or RIPng updates.

**Note:** This feature is useful for situations where a high-speed router is sending updates to a low-speed router.

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

## 1.21.6 Examples

The following example adds a delay time of **15** milliseconds between the sending of updates for the RIP instance, **rip001:**

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#output-delay 15
```

## 1.22 over-subscription-factor

```
over-subscription-factor percent

no over-subscription-factor
```

### 1.22.1 Purpose

For Constrained Shortest Path First (CSPF), specifies the factor by which the bandwidth can exceed the subscribed amount for Resource Reservation Protocol (RSVP)-enabled interfaces.

### 1.22.2 Command Mode

- RSVP router configuration

### 1.22.3 Syntax Description

| | |
|---|---|
| *percent* | Percentage by which the bandwidth may exceed the subscribed amount for RSVP-enabled interfaces. The range of values is 1 through 4294967295. |

### 1.22.4 Default

100 percent.

### 1.22.5 Usage Guidelines

Use the **over-subscription-factor** command to specify the factor by which the bandwidth can exceed the subscribed amount for RSVP-enabled interfaces. This factor is multiplied by the available bandwidth to reserve the oversubscription amount. For example, if the hardware bandwidth for a Fast Ethernet port is 100 mbps and the oversubscription factor is 150 percent, the reserved bandwidth is 150 mbps. If you do not specify a bandwidth, the reserved bandwidth (the default value) is available. If bandwidth has been explicitly reserved (using the **bandwidth** command in RSVP interface configuration mode), that setting overrides this calculation.

To undersubscribe RSVP-enabled interfaces, set a value below 100 percent. To oversubscribe RSVP-enabled interfaces, set a value above 100 percent.

**Note:** The **bandwidth** command in the RSVP interface configuration mode overrides the **over-subscription-factor** command for the particular interface.

Use the **no** form of this command to remove the oversubscription-factor bandwidth value.

## 1.22.6 Examples

The following example shows how to configure the oversubscription-factor on an interface to `110 percent:`

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#over-subscription-factor 110
```

# 1.23 over-subscription-rate

```
over-subscription-rate rate
```

```
no over-subscription-rate
```

```
default fault over-subscription-rate
```

## 1.23.1 Purpose

Specifies the oversubscription rate allowed on an Asynchronous Transfer Mode (ATM) OC port.

## 1.23.2 Command Mode

- ATM OC configuration

## 1.23.3 Syntax Description

| | |
|---|---|
| *rate* | Over-subscription rate as a percentage. The range of values is 0 to 10,000%; the default value is unlimited. |

## 1.23.4 Default

The default rate is unlimited.

## 1.23.5 Usage Guidelines

Use the **over-subscription-rate** command to specify the oversubscription rate allowed on an ATM OC port.

A rate of 0% allows permanent virtual circuits (PVCs) to be created on the port up to the bandwidth of the port; a rate of 1,000% allows PVCs to be created on the port up to the bandwidth of the port +1000%.

Use the **no** form of this command to specify a rate of 0%.

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

### 1.23.6 Examples

The following example shows how to specify an oversubscription rate of 100% for port **1** of the ATM OC-3c/STM-1c line card in slot **4:**

```
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#over-subscription-rate 100
```

With framing bits taken into account, the ATM OC-3c/STM-1c port has a bandwidth of 149.76 Mbps. With an oversubscription rate of 100%, PVCs can be created up to a bandwidth of 299.52 Mbps on this port.

# 1.24 p2p-port

```
p2p-port

no p2p-port
```

## 1.24.1 Purpose

Treats the associated port as always connected to a point-to-point link.

## 1.24.2 Command Mode

- spanning-tree profile configuration

## 1.24.3 Syntax Description

This command has no keywords or arguments.

## 1.24.4 Default

Depending on the type of port, the port is treated as either a full-duplex or half-duplex link.

## 1.24.5 Usage Guidelines

Use the `p2p-port` command to treat the associated port as always connected to a point-to-point link; that is, enable the port for full-duplex operation.

## 1.24.6 Examples

The following example illustrates how the **`spanning-tree profile`** command creates the spanning-tree profile **womp** and enables it for point-to-point linking. In the second part of the example, an Ethernet port is assigned the spanning-tree profile **womp** and, therefore, is enabled for point-to-point linking:

```
[local]Redback(config)#spanning-tree profile womp
[local]Redback(config-stp-prof)#p2p-port
[local]Redback(config-stp-prof)#exit
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#spanning-tree profile womp
```

# 1.25 paired-mode

```
paired-mode subscriber [over-subscription rate]
[port-limit port-limit]
```

```
no paired-mode
```

```
no paired-mode subscriber port-limit
```

```
no pair-mode subscriber
```

```
no pair-mode port-limit
```

## 1.25.1 Purpose

Controls the number of users connected to the same IP address and limits the number of available ports for a subscriber to keep fair usage of the same IP address.

## 1.25.2 Command Mode

NAT pool configuration

## 1.25.3 Syntax Description

| | |
|---|---|
| `subscriber` | Defines paired-mode parameters for subscribers. |
| `over-subscription` *rate* | Optional. Controls the number of users connected to the same IP address. You can apply 1 to 65,535 ports to a full IP address. If oversubscription is applied to an IP address with less than 65,535 ports available, the number of users is scaled down equally.<br>When the number of users exceeds the oversubscription ratio, the system attempts to service subscribers exceeding this threshold.<br>If oversubscription port limit are set, oversubscription uses 16 as the default value. This default value does not displayed in the configuration. |
| `port-limit` *limit* | Optional. Limits the number of available ports for a subscriber to keep fair usage of the same IP address. In some cases, the port limit exceeds the specified limit. The port range limit is 1 through 65,535. |

**Note:** You must configure either `over-subscription` or `port-limit`, or both. If you configure oversubscription only, no port limit is configured. If you configure the port limit only, the oversubscription is calculated to equally share the IP address with the oversubscription = available ports / port limit.

## 1.25.4 Default

The oversubscription is 16 and there are no restrictions on port usage.

### 1.25.5 Usage Guidelines

The oversubscription rate is based on the parameters specified by the **`paired-mode subscribers`** command and the number of configured port-blocks for an IP address. When only the port limit is configured, oversubscription is calculated as follows:

- The actual oversubscription = available ports divided by the port limit
- The oversubscription rate is rounded down. For example, if the rate is less then 1, the system sets the rate to 1.

The available ports are calculated as follows:

- available ports = the number of port-blocks * 4096
- Excluded ports are not included in this calculation.
- When oversubscription is configured, the actual oversubscription = oversubscription * 16 divided by the number of port blocks, is rounded down. For example, if the oversubscription is less then 1, the system sets it to 1.

### 1.25.6 Examples

The following example shows you how to configure paired-mode.

```
[local]Redback(config-ctx)#ip nat pool ?
  WORD  NAT pool name
[local]rock1200(config-ctx)#ip nat pool test ?
  napt  Configure NAPT pool
  <cr>
[local]rock1200(config-ctx)#ip nat pool test napt ?
  logging      Configure logging pool
  multibind    Configure NAPT multibind pool
  paired-mode  Configure paired pool
  <cr>
[local]rock1200(config-ctx)#ip nat pool test napt paired-mode ?
  logging  Configure logging pool
  <cr>
[local]rock1200(config-ctx)#ip nat pool test napt paired-mode logging
[local]rock1200(config-nat-pool)#?
  abort            Abort this configuration - backout from running config
  address          Define NAT pool of ip addresses
  commit           Commit configuration transactions to running config
  exit             Exit nat pool configuration mode
  logging-profile  Define logging-profile parameters
  no               Disable or remove a parameter
  paired-mode      Define paired-mode parameters
  show             Show configuration or system information
[local]rock1200(config-nat-pool)#paired-mode ?
  subscriber  Define paired-mode parameters for subscribers
[local]rock1200(config-nat-pool)#paired-mode subscriber ?
  over-subscription  Define oversubscription ratio
  port-limit         Define port limit
[local]rock1200(config-nat-pool)#paired-mode subscriber over-subscription ?
  1..65535    Define oversubscription ratio
  port-limit  Define port limit
  <cr>
[local]rock1200(config-nat-pool)#paired-mode subscriber over-subscription 64
[local]rock1200(config-nat-pool)#paired-mode subscriber port-limit ?
  1..65535  Define port limit
[local]rock1200(config-nat-pool)#paired-mode subscriber port-limit 4096
```

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 64
   address 100.100.100.1 to 100.100.100.10 port-block 0 to 7  <-8 blocks configured
```

*Example 1     Oversubscription Ratio of 64- and 8-Port-Blocks*

The following example configures 16 users for each IP address, which supports a total of 160 subscribers (16 subscribers x 10 IP addresses). The configuration uses the default oversubscription ratio of 16.

```
context nat_context
ip nat pool nat-pool-paired napt paired
   address 100.100.100.1 to 100.100.100.10
```

*Example 2     Configure 16 Subscribers for Each IP Address*

The following example uses port-blocks to segment an IP addresses. Here each record has 4 port-blocks from an IP address range. Each port-block contains 4096 ports (4 port-blocks allocate16K ports). While CGNAT handles records, it cannot determine if those port-blocks that are not part of the current record are part of the same pool, or that if they belong to another pool. As result, the over subscription ratio calculation is based only on the actual record, and the configured oversubscription is scaled down. If an IP address is configured this way the overall result will be the same, each IP address will have 64 subscribers.

```
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber oversubscription 64
   address 100.100.100.1 to 100.100.100.10 port-block 0 to 3
   address 100.100.100.1 to 100.100.100.10 port-block 4 to 7
   address 100.100.100.1 to 100.100.100.10 port-block 8 to 11
   address 100.100.100.1 to 100.100.100.10 port-block 12 to 15
```

*Example 3     Segmenting an IP Address Using port-blocks*

This example allows 64 users to share the same external IP address. Since there are no more the IP addresses in the pool, the software will allow any number of subscribers on this IP address (it would exceed the oversubscription ratio) since there is no other choice (there is only one IP configured address). If there were other IP addresses configured in the pool, CGNAT will not try to exceed the oversubscription ratio.

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 64
   address 100.100.100.1/32
nat policy pol-nat enhanced
 ! Default class
   pool nat-pool-paired local
```

The following example ensures that none of the users can use no more than 1024 port at the same time. The oversubscription ratio is 64 (65536/1024). 65536 / 1024 = 'full-port-range' / 'port-limit'.

Here 65536 stands for the number of ports an IP address has (0-65535 ports). 'port-limit 1024' indicates that no subscriber can use more than 1024 ports at the same time. If the oversubscription ratio is not set but the port-limit is set, NAT sets the oversubscription ratio to 65536 / 'port-limit' instead of using the default value, 16, because this gives the maximum number of subscriber that can be serviced without running out of ports.

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber port-limit 1024
   address 100.100.100.1/32
   address 100.100.100.2/32
nat policy pol-nat enhanced
   ! Default class
   pool nat-pool-paired local
```

*Example 4     Oversubscription ratio is set 64 and port limit set 1024 ports*

This example shows a port-block ranges for a IP address `100.100.100.2/32`. The number of connected subscribers of `100.100.100.1 is 32`, for `100.100.100.2` is 8, which has 4 port-blocks.

In this case IP address `100.100.100.1` is shared by 32 subscribers, while `100.100.100.2` is shared by 8 users, so each user can have 2048 ports, although it is not guaranteed if the port limit is not specified. The port-block configuration contains 4 blocks. Each port-block contains 4096 ports. 4 port-blocks allocate 16384 ports. 16348 divided by the number of subscribers, 8, allocates 2048 ports to each subscriber. .

If the port limit is not specified, one subscriber can use up all the ports not leaving free ports for the other users. As a result, we highly recommend that you configure the port limit to keep faired usage of the ports.

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 32
   address 100.100.100.1/32  <- Shared by 32 subscribers.
   address 100.100.100.2/32 port-block 1 to 4 <- Shared by 8 users.
```

The above example with also the **`port-limit`** command is shown in the following example: This example shows 32 (65536/2048) subscribers that are sharing the IP address `100.100.100.1` and 8 (4*4096/2048) users are sharing `100.100.100.2`, but the difference is that each subscriber is limited to 2048 ports while the limit for the first configuration is the available ports in the IP, thus the limit is 65536 for the users of `100.100.100.1` and 16384 for the users of `100.100.100.2`.

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber port-limit 2048
   address 100.100.100.1/32
   address 100.100.100.2/32 port-block 1 to 4
```

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 32 port-limit 4096
   address 100.100.100.1/24
nat policy pol-nat enhanced
   ! Default class
   pool nat-pool-paired local
```

In this example the actual number of connected users of `100.100.100.1` is `16`, for `100.100.100.2` is `4`.

```
context nat_context
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 16
   address 100.100.100.1/32
   address 100.100.100.2/32 port-block 1 to 4
```

In the following example, there are 1000 subscribers and the oversubscription ratio is set. The ratio allows up to 64 users for each IP address. The are 10 IP addresses so the oversubscription configuration supports 640 subscribers. When all the IP addresses become full (640 subscribers), the remaining subscribers (360) are distributed evenly among the IP addresses. As a result, , each IP address will have 100 subscribers. The load balancing depends what the oversubscription configuration for an IP address. The bigger the port range of an IP is, the more subscribers it will get. If an IP has only 4 port-blocks (address `100.100.100.2/32` port-block 0 to 3), the address will have 4 times less remainders than an IP address with full range, which contains 16 blocks.

```
ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 64
   address 100.100.100.1 to 100.100.100.10 < 64 subscribers x 10 IP addresses = 640 subscriberss
```

*Example 5    Exceeding Oversubscription Ratio*

In the following example, there are 100 subscribers. The first IP address can hold 64 users while the second IP address can hold 16 users. The 20 subscribers that exceed the over subscription ratio are even distributed between IP Ip address. 16 of these subscribers will use the first IP address, 100.100.100.1/32. The other 4 subscribers will use the second IP address, 100.100.100.2/32.

```
 ip nat pool nat-pool-paired napt paired
   paired-mode subscriber over-subscription 64
   address 100.100.100.1/32  <-equivalent to configuring a port block of 0 to 15, the full range
   address 100.100.100.2/32 port-block 0 to 3 <-Configures 4 blocks
```

*Example 6    100 subscribers*

## 1.26 packet-interval

**packet-interval** ***packet-interval***

**no packet-interval** ***packet-interval***

### 1.26.1 Purpose

Specifies the sampling interval for packets.

### 1.26.2 Command Mode

flow IP sampling configuration

### 1.26.3 Syntax Description

| | |
|---|---|
| *packet-interval* | Rate at which packets are sampled. Range is from 1 to 16383 packets. |

### 1.26.4 Default

None.

### 1.26.5 Usage Guidelines

Use the **packet-interval** command to specify the sampling interval for packets. When random sampling is enabled with the sampling command, statistics are gathered for packets based on the packet interval. For example, if you configured the packet interval to be 9, then statics are gathered for one random packet out of every nine packets. The sampling counter restarts when the ninth packet is processed.

### 1.26.6 Examples

The following example shows how to use the **packet-interval** command to configure the sampling interval to be 100. In this example, statistics are gathered for one random packet out of every 100 packets:

```
[local]Redback# configure
[local]Redback(config)# flow ip sampling
[local]Redback(config-flow-ip-sampling)# packet-interval 100
```

# 1.27 parameter

To specify a field that can have a single value in the definition of an attribute, the syntax is:

**`parameter value`** ***`param-name`*** [***`default-value`***]

**`no parameter`** ***`param-name`***

To specify a field that can have multiple values, the syntax is:

**`parameter list`** ***`param-name`*** [***`default-value`***[**`,`** ***`default-value-2`***[**`,`**....]]]

**`no parameter`** ***`param-name`***

## 1.27.1 Purpose

Specifies a field in a service condition that can be dynamically changed.

## 1.27.2 Command Mode

- service profile configuration

## 1.27.3 Syntax Description

| | |
|---|---|
| **`value`** | Specifies that the field has a single value |
| ***`param-name`*** | Name of a field in a service condition. The Remote Authentication Dial-In User Service (RADIUS) server specifies this name when it configures the service condition for the subscriber on the RADIUS server.<br>The ***`param-name`*** can also be any one of the following predefined parameter names that is used to support dynamic class assignment:<br>• %dynamic_class_qos_in—This parameter holds the Quality of Service (QoS) classes for incoming traffic.<br>• %dynamic_class_qos_out—This parameter holds the QoS classes for outgoing traffic.<br>• %dynamic_class_fwd_in—This parameter holds the forwarding classes for incoming traffic.<br>• %dynamic_class_fwd_out—This parameter holds the forwarding classes for outgoing traffic.<br>• %dynamic_class_nat_out—This parameter holds the NAT classes for outgoing traffic. |
| ***`default-value`*** | Optional. The default value for an optional field in a service condition. Not specified if the field is mandatory. |
| **`list`** | Specifies that an array of values is possible for this field. |
| ***`default-value-n,...`*** | Optional. Additional default values separated by commas (,). |

### 1.27.4 Default

No fields are defined in a service profile.

### 1.27.5 Usage Guidelines

Use the **parameter** command to specify a field in a service condition that can be dynamically changed. You can also use the **parameter** command to specify one of the predefined parameter names that is used to support dynamic class assignment. The maximum number of parameter instances in a service profile is 16; a parameter instance is each occurrence of the command in service profile configuration mode and each occurrence of the command for an array of parameter values in parameter array loop configuration mode.

For example, if the parameter value command appears twice in service profile configuration mode and once in parameter array loop configuration mode for a parameter with four values, the number of parameter instances is six.

Specify a value for each ***default-value*** argument if the subscriber configuration on the RADIUS server need not include this field. If the field is mandatory (the value must be specified in the subscriber configuration on the RADIUS server), do not specify a default value.

Use the **attribute** command (in service profile configuration mode) to specify the attribute that includes the field. If the field can have multiple values, use the **foreach** command (in service profile configuration mode) followed by the **attribute** command.

Use the **no** form of this command to remove the field from the service profile.

### 1.27.6 Examples

The following example specifies a mandatory redirect URL field for the HTTP redirect service condition; the field is defined in the HTTP-Redirect-URL VSA, using the **attribute** command (in service profile configuration mode):

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

The following example specifies a mandatory TCP port number field that can have an array of values; the field is defined using the **attribute** command within a loop initiated by the **foreach** command (in service profile configuration mode):

```
[local]Redback(config-ctx)#radius service profile redirect
[local]Redback(config-svc-profile)#parameter list tcp-port
[local]Redback(config-svc-profile)#
```

The following example specifies default values for the TCP port number field; in this case, the TCP port number is optional and need not be specified by the RADIUS server:

```
[local]Redback(config-ctx)#radius service profile redirect
[local]Redback(config-svc-profile)#parameter list tcp-port www, 443, 8080
[local]Redback(config-svc-profile)#
```

The following example predefines classes “D1 D2 D4 D5” using the parameter %dynamic_class_qos_in and creates a reference to the predefined classes using the class_bearer variable:

```
[local]Redback(config-ctx)#radius service profile dyn-service
[local]Redback(config-svc-profile)#parameter value %dynamic_class_qos_in
“D1 D2 D4 D5”
[local]Redback(config-svc-profile)#parameter value class_bearer
%dynamic_class_qos_in
```

## 1.28 parent-class

**`parent-class`** *`class-name`*

**`no parent-class`** *`class-name`*

### 1.28.1 Purpose

Maps a specific child class to a parent class.

### 1.28.2 Command Mode

- policy group class configuration

### 1.28.3 Syntax Description

| | |
|---|---|
| *`class-name`* | An alphanumeric string of up to 39 characters that specifies the name of a parent class. |

### 1.28.4 Default

The mapping of a child class to a parent class is not specified.

### 1.28.5 Usage Guidelines

Use the **`parent-class`** command to map a metering or policing policy class to a class specified in another metering or policing policy. The class mapping configuration is employed when applying a hierarchical metering or policing policy to traffic on a child circuit that has its own metering and policing policy. Using the class mapping, the SmartEdge router determines the parent policy class for treating the child class traffic when enforcing the parent metering or policing policy. For more information about the mapping of the ACL class or a class-definition map class to a parent policy class, see *Mapping a Child Policy Class to a Parent Class* in *Configuring Rate-Limiting and Class-Limiting*.

Use the **`no`** form of this command to remove the mapping of the child class to the parent class.

### 1.28.6 Examples

The following example shows how to map a child class to a parent class. In this example, the child class voip is mapped to the parent class high and the child class data is mapped to the parent class low:

```
[local]Redback(config)#qos policy child-pol metering
[local]Redback(config-policy-metering)#ip access-group child-acl local
[local]Redback(config-policy-group)#class voip
[local]Redback(config-policy-group-class)#parent-class high
[local]Redback(config-policy-group-class)#rate 50 burst 100
[local]Redback(config-policy-class-rate)#class data
[local]Redback(config-policy-group-class)#parent-class low
[local]Redback(config-policy-group-class)#rate 20 burst 40
```

# 1.29 partition

**partition** ***name*** **[size** ***size_value*****] [disk** ***disk_num*****] [non-mirror]**

**no partition** ***name***

## 1.29.1 Command Mode

SSE group configuration

## 1.29.2 Syntax Description

| | |
|---|---|
| ***name*** | Name of the partition. |
| **size** ***size_value*** | Configures the size of the partition, in gigabytes (GB). Required when creating a new partition. Range: 1 to 4,294,967,295. |
| **disk** ***disk_num*** | Disk number on the SSE card. Values: 1 or 2. Assigns the partition to an SSE disk when operated independently. Applies to network-redundant SSE groups only, where **raid-0** is not configured. Required when creating a new partition on a network-redundant SSE group. |
| **non-mirror** | By default, partition data is mirrored to the standby. The **non-mirror** keyword specifies that the partition should not mirror the data to the standby if redundancy is set. Applies to network-redundant SSE groups only. |

## 1.29.3 Default

No partition is configured.

## 1.29.4 Usage Guidelines

Creates the partition and enters SSE partition configuration mode. You can create multiple partitions. The partition name must be unique in the SSE group.

The **disk** and **non-mirror** keywords apply only to network-redundant SSE groups. For other operational settings, the command is rejected if these keywords are specified.

Any partition configured must be fully allocated on the SSE disk for it to be operational.

The no form of the command removes the partition from the SSE group. The partition still exists on the SSE disk and data is maintained. Use the **delete partition sse** ***slot disk_num partition_name*** command in exec mode to remove the partition and all data.

## 1.29.5 Examples

```
[local]Redback(config)#sse group sse_group_1
[local]Redback(config-SE-group)#partition p01 size 5 disk 1
```

## 1.30 passive

**passive**

{**no** | **default**} **passive**

### 1.30.1 Purpose

When entered in OSPF area configuration mode, sets all interfaces configured in the specified Open Shortest Path First (OSPF) area to passive mode.

When entered in OSPF interface or OSPF3 interface configuration mode, sets an OSPF or OSPF Version 3 (OSPFv3) interface to passive mode.

### 1.30.2 Command Mode

- OSPF area configuration
- OSPF interface configuration
- OSPF3 interface configuration

### 1.30.3 Syntax Description

This command has no keywords or arguments.

### 1.30.4 Default

No interfaces are in passive mode.

### 1.30.5 Usage Guidelines

Use the **passive** command in OSPF area configuration mode to set all interfaces configured in the specified OSPF area to passive mode.

**Note:** OSPF passive mode disables OSPF interfaces from sending OSPF packets.

Setting all interfaces in an OSPF area to passive mode is useful for large, pure edge aggregation applications, where there may be hundreds, or perhaps thousands, of customer-facing circuits. To distribute routes for the customer-facing interfaces to the upstream routers, you can enable OSPF on the customer-facing interfaces, and then set them all to passive mode using the **passive** command in OSPF area configuration mode.

Use the **passive** command in OSPF interface or OSPF3 interface configuration mode to set an OSPF or OSPFv3 interface to passive mode.

Use the **no** or **default** form of this command to return the interface, or all interfaces within an OSPF area, to the default state.

## 1.30.6 Examples

The following example sets the **ospf1** interface to passive mode:

```
[local]Redback(config-ospf-area)#interface ospf1
[local]Redback(config-ospf-if)#passive
```

# 1.31 passive-interface

```
passive-interface
```

```
no passive-interface
```

## 1.31.1 Purpose

Configures the Intermediate System-to-Intermediate System (IS-IS) instance to advertise the interface's IP address without actively running IS-IS on the interface.

## 1.31.2 Command Mode

IS-IS interface configuration

## 1.31.3 Syntax Description

This command has no keywords or arguments.

## 1.31.4 Default

Passive mode is disabled.

## 1.31.5 Usage Guidelines

Use the **`passive-interface`** command to configure the IS-IS instance to advertise the interface's IP addresses without actively running IS-IS on the interface.

When an IS-IS interface is configured in passive mode, IS-IS packets are sent and no adjacency is formed on the interface. IS-IS advertises the interface's IP address in its link-state protocol data units (LSPs).

The default metric value for a passive interface is 1. To change the metric value, use the **`metric`** command in IS-IS interface configuration mode.

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

## 1.31.6 Examples

The following example configures the **fa4/1** interface as a passive IS-IS interface:

```
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface fa4/1
[local]Redback(config-isis-if)#passive-interface
```

# 1.32 password

```
password password
```

```
no password
```

## 1.32.1 Purpose

Specifies the authentication password that the subscriber enters when initiating a Point-to-Point Protocol (PPP) session.

## 1.32.2 Command Mode

subscriber configuration

## 1.32.3 Syntax Description

| | |
|---|---|
| *password* | Alphanumeric text string. Control characters are not allowed. |

## 1.32.4 Default

None

## 1.32.5 Usage Guidelines

Use the **password** command to specify the authentication password that the subscriber enters when initiating a PPP session. When using Challenge Handshake Authentication Protocol (CHAP) Password Authentication Protocol (PAP), the password obtained from the subscriber must match the password configured in the corresponding subscriber record. This command is available for individual subscriber records, but not for a default subscriber record.

You can enter a password with embedded spaces by enclosing the entire password in double quotes; for example, "**This is a Password With Spaces**."

Use the **no** form of this command to remove the password from the subscriber's record.

## 1.32.6 Examples

The following example configures a password of **DontTellAnyone:**

```
[local]Redback(config-sub)#password DontTellAnyone
```

# 1.33 password (BGP)

**`password`** ***`password`***

**`no password`**

## 1.33.1 Purpose

Configures an encrypted Message Digest 5 (MD5) password for the Border Gateway Protocol (BGP) neighbor or peer group.

## 1.33.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

## 1.33.3 Syntax Description

| | |
|---|---|
| *`password`* | Alphanumeric string consisting of up to 80 characters. |

## 1.33.4 Default

None

## 1.33.5 Usage Guidelines

Use the **`password`** command to assign an encrypted MD5 password for the BGP neighbor or peer group.

**Note:** For a BGP session to be established, the MD5 password must be the same on both the router and its neighbor.

Use the **`no`** form of this command to remove an assigned password from the BGP neighbor or peer group.

## 1.33.6 Examples

The following example assigns the password **secret** to the external BGP (eBGP) neighbor at IP address **10.10.1.1:**

```
[local]Redback(config-bgp)#neighbor 10.10.1.1 external
[local]Redback(config-bgp-neighbor)#password secret
```

# 1.34 path-trace

**`path-trace`** {**`length`** *`length`* | **`message`** *`text`*}

**`no path-trace message`**

## 1.34.1 Purpose

Specifies either the maximum length of the message or the text string to be traced on an administrative unit-3 (AU-3) or an AU-4 on a channelized STM-1 port.

## 1.34.2 Command Mode

- AU-3 configuration
- STM-1 configuration

## 1.34.3 Syntax Description

| | |
|---|---|
| **`length`** *`length`* | Maximum length of the message, in bytes, according to one of the following keywords:<br>• `16`—Specifies the maximum length of the message to be 15 characters. This is the default length.<br>• `64`—Specifies the maximum length of the message to be 62 characters. |
| **`message`** *`text`* | Text string with up to 62 ASCII characters. |

## 1.34.4 Default

The length is 16 and the message is *Redback*.

## 1.34.5 Usage Guidelines

Use the **`path-trace`** command to specify either the maximum length of the text or the text string to be traced on an AU-3 or AU-4 on a channelized STM-1 port.

If you enter the **`aug-mapping au3`** command (in STM-1 configuration mode), the **`path-trace`** command is no longer available in STM-1 configuration mode; it is available in AU-3 configuration mode.

The first byte in a 16-character message is reserved for the results of a CRC7 calculated on the message.

The final two characters in a 64-character message are reserved for the CR/LF (0x0D/0x0A).

Use the **no** form of this command to set the maximum length to 16, and the message text to *Redback*. You cannot disable the path trace feature for channelized STM-1 ports.

**Note:** The **message** keyword is used without the ***text*** argument in the **no** form of this command.

**Note:** This command is also described in *Configuring ATM, Ethernet, and POS Ports* for ports on Packet over SONET/SDH (POS) and 4-port ATM OC-3c/STM-1c line cards.

### 1.34.6 Examples

The following example shows how to specify a path trace with a maximum message length of **64** and the text string for port **1** of the channelized STM-1 line card in slot **2**; the port is mapped with the default administrative unit group (AUG) mapping, AU-4:

```
[local]Redback(config)#port channelized-stm1 2/1
[local]Redback(config-stm1)#path-trace length 64
[local]Redback(config-stm1)#path-trace this is a test of an extended length message.
```

# 1.35 path-trace (ATM OC, POS, WAN-PHY)

```
path-trace message text

{no | default} path-trace message
```

## 1.35.1 Purpose

Specifies the text string to be traced on a Packet over SONET/SDH (POS), second-generation Asynchronous Transfer Mode (ATM) OC, Channelized OC/STM, or Ethernet WAN-PHY port.

## 1.35.2 Command Mode

- ATM OC configuration
- port configuration

## 1.35.3 Syntax Description

| `message` | Specifies that a text string follows. |
|---|---|
| *`text`* | Text string with up to 62 ASCII characters, depending on the type of port:<br>• POS ports—Maximum length is 62.<br>• Second-generation ATM OC ports with Synchronous Optical Network (SONET) framing—Maximum length is 62.<br>• Second-generation ATM OC ports with Synchronous Digital Hierarchy (SDH) framing—Maximum length is 15.<br>• Ethernet WAN-PHY ports with SONET or SDH framing—Maximum length is 15.<br>• Channelized OC ports with Synchronous Optical Network (SONET) framing—Maximum length is 15.<br>• Channelized OC ports with Synchronous Digital Hierarchy (SDH) framing—Maximum length is 15. |

## 1.35.4 Default

The transmitted text string is *Redback*.

## 1.35.5 Usage Guidelines

Use the `path-trace` command to specify the text string to be on a POS, Channelized POS, second-generation Asynchronous Transfer Mode (ATM) OC, or Ethernet WAN-PHY port.

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

The actual message length is 16 or 64 bytes, with one additional byte required for framing for a 15-character message and two additional bytes required for a 62-character message.

**Note:** For a POS port, you must first enable the path trace, path maintenance, and path alarm monitoring features for the card on which the port is configured, by using the **sonet-eu** command (in card configuration mode). The **sonet eu** command is not needed for ports on a second-generation ATM OC card.

You cannot disable the path trace feature for Ethernet WAN-PHY or second-generation ATM OC line cards; to disable the path trace feature for ports on POS line cards, you must enter the **no** form for the **sonet-eu** command (in card configuration mode).

Use the **show port detail** command (in any mode) to display the path trace length and message.

Use either the **no** or **default** form of this command to specify the default text string.

### 1.35.6 Examples

The following example shows how to enable path trace and specify the text string, `this is a test`, for port `1` on the POS line card in slot `9`:

```
[local]Redback(config)#card oc3e-8-port 9
[local]Redback(config-card)#sonet-eu
[local]Redback(config-card)#exit
[local]Redback(config)#port pos 9/1
[local]Redback(config-port)#path-trace this is a test
```

The following example shows how to enable path trace and specify the text string, `this is a test`, for port the 10ge-1-port line card that has been configured to operate in WAN-PHY mode (slot `2`, port `1`:

```
[local]Redback(config)#card 10ge-1-port 2
[local]Redback(config-card)#exit
[local]Redback(config)#port wan-phy 2/1
Note: Creating a port may cause the card to reload. Commit to
continue; abort to exit without change
[local]Redback(config)#commit
[local]Redback(config-port)#path-trace this is a test
```

# 1.36 pe-type

**pe-type** {**hub** | **spoke**}

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

## 1.36.1 Purpose

Specifies the connection type used between the local and remote provider edge (PE) devices.

## 1.36.2 Command Mode

VPLS profile neighbor configuration

## 1.36.3 Syntax Description

| | |
|---|---|
| **hub** | Hub connection type. This connection type is used if the Virtual Private LAN Services (VPLS) topology is enabled using a full mesh of pseudowire. Packets received on a hub link pseudowire are not forwarded on other hub connections (split horizon). |
| **spoke** | Spoke connection type. This connection type is used for enabling hierarchical VPLS topologies between multitenant unit switch (MTU-s) and PE routers (PE-rs), or when a full mesh of pseudowires is not used. Forwarding in unrestricted on spoke links. |

## 1.36.4 Default

The hub connection type is used.

## 1.36.5 Usage Guidelines

Use the **pe-type** command to specifies the connection type used between the local and remote PE devices. Currently, hub and spoke connection types are supported. For proper VPLS peering, both ends of the peer must be configured with the same connection type.

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

## 1.36.6 Examples

The following example sets the connection type to **spoke:**

```
[local]Redback#config
[local]Redback(config)#vpls profile foo
[local]Redback(config-vpls-profile)#neighbor 10.10.10.1
[local]Redback(config-vpls-profile-neighbor)#pe-type spoke
[local]Redback(config-vpls-profile-neighbor)#
```

# 1.37 peer-as

**peer-as** {*asn* | *nn*:*nn*}

**no peer-as** {*asn* | *nn*:*nn*}

## 1.37.1 Purpose

Configures a peer's autonomous system number (ASN).

## 1.37.2 Command Mode

MSDP peer configuration

## 1.37.3 Syntax Description

| | |
|---|---|
| *asn* | Autonomous system number, in integer format, of the autonomous system that includes the peer. The range of values is 1 to 65,535. The subrange 64,512 to 65,535 is reserved for private autonomous systems. |
| *nn*:*nn* | Optional. ASN, in 4-byte integer format, that includes the peer. With 4-byte integer format, the first *nn* indicates the two higher-order bytes, and the second *nn* denotes the two lower-order bytes. |

## 1.37.4 Default

None

## 1.37.5 Usage Guidelines

Use the **peer-as** command to configure a peer's ASN.

Use the **no** form of this command to delete the source active (SA) number from the peer's configuration.

## 1.37.6 Examples

The following example configures a peer's SA number to **37:**

```
[local]Redback(config-msdp)#peer 192.168.1.1 local-tcp-source ToWan12

[local]Redback(config-msdp-peer)#peer-as 37
```

# 1.38 peer-end-point

**`peer-end-point local`** *`loc-ip-addr`* [**`remote`** *`rem-ip-addr`*] [**`context`** *`ctx-name`*]

**`no peer-end-point`**

## 1.38.1 Purpose

Assigns IP addresses to the tunnel endpoints.

## 1.38.2 Command Mode

tunnel configuration

## 1.38.3 Syntax Description

| | |
|---|---|
| `local` *`loc-ip-addr`* | IP address of the local end of the tunnel. The format is *`A.B.C.D`*. |
| `remote` *`rem-ip-addr`* | Optional. IP address of the remote end of the tunnel. Required except when you have created an overlay tunnel for which you have specified that the system assign the remote IP address. The format is *`A.B.C.D`*. |
| `context` *`ctx-name`* | Optional. Name of the context that contains the interface to the local end of the tunnel. If no context is specified, the interface to the local end of the tunnel is assumed to be in the **local** context. |

## 1.38.4 Default

None

## 1.38.5 Usage Guidelines

Use the **`peer-end-point`** command to assign IP addresses to the tunnel endpoints. This command creates the tunnel between the two endpoints.

**Note:** IP-in-IP and overlay tunnels support a single tunnel circuit in each tunnel; GRE tunnels can support multiple tunnel circuits with the use of keys. For information about GRE tunnel circuits, see *Configuring GRE Tunnels*.

The remote IP address at one end of the tunnel is the same as the local IP address at the other end of the tunnel. If the remote IP address is not adjacent to the local IP address, and the remote site cannot be reached with a routing protocol, you must also enter the **`ip route`** command in context configuration mode.

If you create an overlay tunnel using the **`tunnel`** command with the **`ipv6v4-auto`** keyword, the system assigns an IP address to the remote endpoint. In this case, you do not include the **remote** ***rem-ip-addr*** construct when you enter this command.

The **local** ***loc-ip-addr*** construct must match the IP address of an interface.

If you are creating more than one tunnel, they can use the same IP address for the local endpoint (the IP address assigned to the interface) as long as the remote IP addresses are all different.

To use an interface and its local IP address for more than one tunnel, you must specify the **loopback** keyword with the **interface** command (in context configuration mode) when you create the interface for the tunnels. The **loopback** keyword allows you to reuse the IP address for more than one tunnel.

Use the **no** form of this command to delete this tunnel and any associated parameters that have been specified in tunnel configuration mode. The keywords are not available for the **no** form of this command.

### 1.38.6 Examples

The following example shows how to create an interface, **toDenver**, with a public IP address of **172.16.1.1**; then it creates an overlay tunnel, **DenverTnl**, with a remote IP address of **172.16.1.2** and a local IP address of **172.16.1.1:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface toDenver
[local]Redback(config-if)#ip address 172.16.1.1/30
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#tunnel ipv6v4-manual DenverTnl
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.16.1.2
```

The following example shows how to create two overlay tunnels each using an interface, **LocalEnd**. Both tunnels use the same local IP address; it is assumed that the remote IP address for **Tun2** can be reached with a routing protocol, so the **ip route** command in context configuration mode is not needed:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface LocalEnd loopback
[local]Redback(config-if)#ip address 172.16.1.1/32
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#tunnel Tun1
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.16.1.2
[local]Redback(config-tunnel)#no shutdown
[local]Redback(config-tunnel)#exit
[local]Redback(config-ctx)#tunnel Tun2
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.20.1.2
[local]Redback(config-tunnel-peer)#no shutdown
[local]Redback(config-tunnel-peer)#end
```

# 1.39 peer-group

For BGP router configuration mode, the command syntax is:

**`peer-group`** ***`group-name`*** {**`external`** | **`internal`**}

**`no peer-group`** ***`group-name`*** {**`external`** | **`internal`**}

For BGP neighbor configuration and BGP neighbor address family configuration modes, the command syntax is:

**`peer-group`** ***`group-name`***

**`no peer-group`** ***`group-name`***

## 1.39.1 Purpose

When entered in BGP router configuration mode, configures an internal Border Gateway Protocol (iBGP) or external BGP (eBGP) peer group and enters BGP peer group configuration mode.

When entered in BGP neighbor configuration or BGP neighbor address family configuration mode, applies the attributes of a configured peer group to a BGP neighbor or BGP neighbor address family.

## 1.39.2 Command Mode

- BGP neighbor address family configuration
- BGP neighbor configuration
- BGP router configuration

## 1.39.3 Syntax Description

| | |
|---|---|
| *`group-name`* | Name of the peer group. |
| **`external`** | Configures an eBGP peer group. |
| **`internal`** | Configures an iBGP peer group. |

## 1.39.4 Default

There are no preconfigured peer groups. Once a peer group is configured, it is enabled.

## 1.39.5 Usage Guidelines

Use the **peer-group** command in BGP router configuration mode to configure an iBGP or eBGP peer group and enter BGP peer group configuration mode.

Peer groups are helpful in cases where many BGP neighbors are configured with the same outbound update policies. Grouping a large number of neighbors into one or more peer groups simplifies modifications to a configuration, and more importantly, makes BGP update generation more efficient. The use of peer groups is strongly recommended when there are a large number of peers.

**Note:** BGP peer groups can be configured in standard contexts and VPN contexts.

You can apply attributes to BGP neighbors or BGP address families. Attributes that are not configurable for peer groups are those set by the following commands in BGP neighbor configuration mode: **accept prefix-filter**, **local-as**, and **remote-as**.

Use the **peer-group** command in BGP neighbor configuration mode to apply the characteristics of a peer group to one or more BGP neighbors. A neighbor can be assigned to a peer group only if the neighbor and the peer group is of the same type—external or internal BGP. If a neighbor belongs to a particular peer group, it cannot be configured to belong to another peer group. The previous peer group membership must first be explicitly deleted before the peer membership can be reconfigured.

Attributes are inherited from the peer group to which a neighbor is assigned. The following BGP neighbor configuration mode commands represent attributes that cannot be customized per neighbor when the neighbor is assigned to a peer group: **advertisement-interval**, **ebgp-multihop**, **local-as**, **send community**, and **timers**. Attributes inherited from a peer group that can be customized per neighbor include those set by the following commands: **description**, **password**, **send prefix**, **shutdown**, and **update-source**.

Use the **peer-group** command in BGP neighbor address family configuration mode to apply the characteristics of a peer group to one or more BGP neighbor address families. A BGP neighbor address family can belong to more than one peer group and can be modified to belong to a different peer group without having to delete the previous peer group association first.

Attributes are inherited from the peer group to which a BGP neighbor address family is assigned. The following commands in BGP neighbor address family configuration mode represent attributes that cannot be customized per address family once it is assigned to a peer group: **as-path-list out**, **prefix-list out, remove-private-as**, and **route-map out**. Attributes inherited from a peer group that can be customized per neighbor address family include those set by the following commands: **as-path-list in**, **default-originate**, **maximum-prefix**, **prefix-list in**, and **route-map in**.

By default, a configured peer group is automatically enabled. To disable a peer group, enter the **shutdown** command in BGP peer group configuration mode.

Use the **no** form of this command to remove a peer group.

## 1.39.6 Examples

The following example assigns the BGP neighbor at IP address **10.1.1.1** to the peer group **pgrp-101**. The BGP neighbor at IP address **10.1.1.1** inherits all of its configuration from peer group **pgrp-101**. The configuration also assigns the BGP neighbor at IP address **10.2.2.2** to the peer group **pgrp-200**. The BGP neighbor at IP address **10.2.2.2** inherits all outbound routing policies and the properties of the **remove-private-AS** command from peer group **pgrp-200**, but does not inherit the group's inbound policies or description information:

```
[local]Redback(config-ctx)#router bgp 101
[local]Redback(config-bgp)#peer-group pgrp-101 internal
[local]Redback(config-bgp-peer-group)#description config IBGP neighbors
[local]Redback(config-bgp-peer-group)#password encrypted 8F733D8CD3F98AE0
[local]Redback(config-bgp-peer-group)#update-source interface1
[local]Redback(config-bgp-peer-group)#next-hop-self
[local]Redback(config-bgp-peer-group)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#maximum prefix 20000
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-peer-group)#exit
[local]Redback(config-bgp)#peer-group pgrp-200 external
[local]Redback(config-bgp-peer-group)#ebgp-multihop 10
[local]Redback(config-bgp-peer-group)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#as-path-list aspath-in in
[local]Redback(config-bgp-peer-af)#as-path-list aspath-out out
[local]Redback(config-bgp-peer-af)#remove-private-AS
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-peer-group)#exit
[local]Redback(config-bgp)#neighbor 10.1.1.1 internal
[local]Redback(config-bgp-neighbor)#peer-group pgrp-101
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 10.2.2.2 external
[local]Redback(config-bgp-neighbor)#peer-group pgrp-200
[local]Redback(config-bgp-neighbor)#remote-as 200
[local]Redback(config-bgp-neighbor)#description neighbor at corpA
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#as-path-list as-in in
[local]Redback(config-bgp-peer-af)#as-path-list as-out out
[local]Redback(config-bgp-peer-af)#route-map rtmap-out out
```

# 1.40 peer id

**peer id** ***peer-name***

**no peer id** ***peer-name***

## 1.40.1 Purpose

Filters incoming new neighbor connections using the sender name of the incoming Access Node Control Protocol (ANCP) neighbor peer.

## 1.40.2 Command Mode

- ANCP neighbor configuration

## 1.40.3 Syntax Description

| | |
|---|---|
| ***peer-name*** | Name of an ANCP neighbor peer. |

## 1.40.4 Default

If a peer name is not specified for this profile, there is no restriction on the sender name in a received General Switch Management Protocol (GSMP) adjacency protocol message from an ANCP neighbor peer.

## 1.40.5 Usage Guidelines

Use the **peer id** command to filter incoming new neighbor connections using the sender name of the incoming ANCP neighbor peer. The sender name is in the GSMP adjacency protocol message from the ANCP neighbor peer.

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

## 1.40.6 Examples

The following example specifies a name for an ANCP neighbor peer:

```
[local]Redback(config-ancp-neighbor)#peer id 01:02:03:04:05:06
```

# 1.41 peer ip-address

**`peer ip-address`** ***`ip-addr`***

**`no peer ip-address`** ***`ip-addr`***

## 1.41.1 Purpose

Filter incoming new neighbor connections using the IP address of the incoming Access Node Control Protocol (ANCP) neighbor peer.

## 1.41.2 Command Mode

- ANCP neighbor configuration

## 1.41.3 Syntax Description

| | |
|---|---|
| *`ip-addr`* | IP address of an ANCP neighbor peer. |

## 1.41.4 Default

If an IP address is not specified for this profile, there is no restriction on the IP address in a received General Switch Management Protocol (GSMP) adjacency protocol message from an ANCP neighbor peer.

## 1.41.5 Usage Guidelines

Use the **`peer ip-address`** command to filter incoming new neighbor connections using the IP address of the incoming ANCP neighbor peer. The incoming IP address is matched against the specified IP address and the connection rejected if there is no match.

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

## 1.41.6 Examples

The following example specifies IP address for an ANCP neighbor peer:

```
[local]Redback(config-ancp-neighbor)#peer ip-address 30.100.1.20
```

# 1.42 peer (L2TP)

**peer name** ***l2tp-peer-name*** {**preference** ***priority*** | **weight** ***weight***}

**no peer name** ***l2tp-peer-name***

## 1.42.1 Purpose

Adds an existing peer to the current Layer 2 Tunneling Protocol (L2TP) group.

## 1.42.2 Command Mode

L2TP group configuration

## 1.42.3 Syntax Description

| | |
|---|---|
| **name** ***l2tp-peer-name*** | Name of the peer to be added to the current L2TP group. |
| **preference** ***priority*** | Priority for the priority algorithm when assigning sessions to this peer. |
| **weight** ***weight*** | Weight for the weighted-round-robin algorithm when assigning sessions to this peer. |

## 1.42.4 Default

No peer is added to the current L2TP group.

## 1.42.5 Usage Guidelines

Use the **peer** command to add an existing peer to an L2TP group. The ***l2tp-peer-name*** argument is the peer name specified in the l2tp-peer command in context configuration mode or its domain alias, specified by the **domain** command in L2TP peer configuration mode.

Use the **preference** ***priority*** construct to override the implicit priority for the peer, if you have specified the **priority** keyword in the **algorithm** command (in L2TP group configuration mode). Otherwise, the implicit priority is the order in which the **peer** commands are run, with the first peer entered having the highest priority.

If you have specified the **weighted-round-robin** keyword in the **algorithm** command (in L2TP group configuration mode), use the **weight** ***weight*** construct to assign a weight for the peer to be used in the calculation of the priority.

This command takes effect immediately, but does not affect Point-to-Point Protocol (PPP) sessions that are already established; only future PPP sessions.

Use the **no** form of this command to remove the named peer from the group.

### 1.42.6 Examples

The following example shows how to select (or create) an L2TP group, add three L2TP peers to the group, sets the algorithm to strict priority, and set the deadtime to 5 minutes:

```
[local]Redback(config-ctx)#l2tp-group name group1
[local]Redback(config-l2tp-group)#algorithm priority
[local]Redback(config-l2tp-group)#peer name sweet1 preference 10
[local]Redback(config-l2tp-group)#peer name sweet2 preference 20
[local]Redback(config-l2tp-group)#peer name sweet3 preference 30
[local]Redback(config-l2tp-group)#default deadtime
```

# 1.43 peer (L2VPN profile)

**peer** *peer-addr*

## 1.43.1 Purpose

Specify the IP address of the peer router that can be reached through the LSPs on the current router and enter L2VPN profile peer configuration mode.

## 1.43.2 Command Mode

- L2VPN profile configuration

## 1.43.3 Syntax Description

| | |
|---|---|
| *peer-addr* | IP address of the peer router. |

## 1.43.4 Default

none.

## 1.43.5 Usage Guidelines

Use the **peer** command to specify the IP address of the peer router that can be reached through the LSPs on the current router and enter L2VPN profile peer configuration mode.

## 1.43.6 Examples

The following example shows how to specify the IP address of the peer router in an L2VPN profile called `pr1`:

```
[local]Redback(config)#l2vpn profile pr1
Redback(config-l2vpn-xc-profile)peer 111.111.111.111
Redback(config-l2vpn-xc-profile-peer)
```

# 1.44 peer (MSDP)

**peer** *peer-addr* **local-tcp-source** *if-name*

**no peer** *peer-addr* **local-tcp-source** *if-name*

## 1.44.1 Purpose

Configures an Multicast Source Discovery Protocol (MSDP) peer and enters MSDP peer configuration mode.

## 1.44.2 Command Mode

MSDP router configuration

## 1.44.3 Syntax Description

| *peer-addr* | IP address of the router that is to be the MSDP peer. |
|---|---|
| **local-tcp-source** *if-name* | Name of the interface whose address becomes the source IP address for Transmission Control Protocol (TCP) connection. |

## 1.44.4 Default

None

## 1.44.5 Usage Guidelines

Use the **peer** command to configure an MSDP peer and enter MSDP peer configuration mode for peer-specific configurations.

Use the **no** form of this command to delete an MSDP peer.

## 1.44.6 Examples

The following example configures a router with an IP address of **192.168.1.1** to be an MSDP peer that uses the **ToWan12** interface for the TCP connection:

```
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#peer 192.168.1.1 local-tcp-source ToWan12
[local]Redback(config-msdp-peer)#
```

## 1.45 peer (NTP)

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

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

### 1.45.1 Purpose

Configures an NTP peer for a context.

### 1.45.2 Command Mode

NTP server configuration

### 1.45.3 Syntax Description

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

### 1.45.4 Default

There is no NTP peer enabled in the context.

### 1.45.5 Usage Guidelines

To configure the system clock to synchronize a peer or to be synchronized by a peer, enable an NTP server in a context with the **peer** command.

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

### 1.45.6 Examples

The following example configures an NTP peer in the **isp202** context:

```
[local]Redback(config)#context isp202
[local]Redback(config-ctx)#ntp-mode
[local]Redback(config-ntp-server)#peer 1.1.1.5 version 3 source ntp
```

# 1.46 periodic

**periodic** *day...* *hh*:*mm* **to** *hh*:*mm* {{**permit** | **deny**} | **class** *class-name*}

**no periodic** *day...* *hh*:*mm* **to** *hh*:*mm*

## 1.46.1 Purpose

Creates a periodic time access control list (ACL) condition statement.

## 1.46.2 Command Mode

ACL condition configuration

## 1.46.3 Syntax Description

| | |
|---|---|
| *day...* | One or more days of the week in which the ACL condition is applied. |
| *hh*:*mm* | Hour and minute, for each specified day of the week, to start the ACL condition. |
| to *hh*:*mm* | Hour and minute, for each specified day of the week, to stop the ACL condition. |
| permit | Applies permit action, during the specified time ranges, to all ACL statements that reference the ACL condition. |
| deny | Applies deny action, during the specified time ranges, to all ACL statements that reference the ACL condition. Used only with IP ACLs. |
| class *class-name* | Name of the class assigned to policy ACL statements that reference the ACL condition. Used only with policy ACLs. |

## 1.46.4 Default

None

## 1.46.5 Usage Guidelines

Use the **periodic** command to create a periodic time ACL condition statement that permits or denies packets, or assigns packets to a class, based on specific date and time ranges. A periodic time ACL condition is referenced by either an IP ACL statement or a policy ACL statement.

Each ACL condition statement can include up to seven absolute or periodic time statements in any combination.

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

### 1.46.6 Examples

The following example creates a periodic ACL condition statement for the ACL condition, **55**, which is referenced by the policy ACL, **policy_acl_2**, such that the **Bar003** class name is applied every Wednesday from 9:00 p.m. to 11:00 p.m (21:00 to 23:00 in 24-hour format) to packets assigned to the **Bar003** class:

```
[local]Redback(config-ctx)#policy access-list policy_acl_2
[local]Redback(config-access-list)#condition 55 time-range
[local]Redback(config-acl-condition)#periodic wednesday 21:00 to 23:00 class Bar003
```

# 1.47 permit (IPv4 ACL)

Statements in IPv4 and IPv6 ACLs can contain different criteria; for syntax for statements for IPv6 ACLs, see permit (IPV6 ACL).

**permit** [*protocol*] {*src src-netmask* | **any** | **host** *src*} [{*cond port* | **range** *port end-port*}] [**max-sessions** *limit*] [**min-sessions** *limit*] [*dest dest-netmask* | **any** | **host** *dest*] [*cond port* | **range** *port end-port*] [**length** {*cond length* | **range** *length end-length*}] [**icmp-type** *icmp-type* [**icmp-code** *icmp-code*]] [**igmp-type** *igmp-type*] [**dscp eq** *dscp-value*] [**established** | **setup** | **invalid-tcp-flags**] [**precedence** *prec-value*] [**tos** *tos-value*] [[**fragments**] | [**ip-options**]] [**class** *class-name*] [**condition** *cond-id*]

{**no** | **default**} **permit** *src src-wildcard*

## 1.47.1 Purpose

Creates an IP or policy access control list (ACL) statement to allow packets that meet the specified criteria.

## 1.47.2 Command Mode

access control list configuration

## 1.47.3 Syntax Description for IPv4 Statements

| | |
|---|---|
| *protocol* | Optional. Number indicating a protocol as specified in RFC 1700, *Assigned Numbers*. The range of values is 0 to 255 or one of the keywords listed in Table 8. |
| *src* | Source address to be included in the permit or deny criteria. An IP address in the form *A.B.C.D*. |
| *src-netmask* | Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the *src-wildcard* argument must be matched by the corresponding bits in the *src* argument. For any one-bits in the *src-wildcard* argument, the corresponding bits in the *src* argument are ignored. |
| **any** | Specifies a completely wildcarded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255. |
| **host** *source* | Address of a single-host source with no wild-card address bits. The **host** *source* construct is identical to the *src src-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0). |
| *cond* | Optional. Matching condition for the *port* or *length* argument, according to one of the keywords listed in Table 9. |
| *port* | Optional. Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source or destination port. This argument is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 10 and Table 11. |

| | |
|---|---|
| **range** ***port end-port*** | Optional if you specify the TCP or UDP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must be within the specified range to match the criteria. The range of values is 1 to 65,535 or one of the keywords listed in Table 10 and Table 11. |
| **max-sessions** ***limit*** | Optional. Maximum number of sessions allowed for the specified IP address or IP subnet. This construct is only available for TCP. Use the **ip access-list** command with the **ssh-and-telnet-acl** keyword to apply an IP ACL to packets associated with an Secured Shell (SSH) or a Telnet server. The range of values is 1 to 32. |
| **min-sessions** ***limit*** | Optional. Minimum number of sessions allowed for the specified IP address or IP subnet. This construct is only available if you specify TCP as the protocol in this command and use the **ip access-list** command with the **ssh-and-telnet-acl** keyword to apply an IP ACL to packets associated with an SSH or a Telnet server. The range of values is 0 to 32.<br>The sum of values specified for the **min-sessions** ***limit*** construct for all specified IP addresses or IP subnets must not exceed 32. |
| ***dest*** | Optional. Destination address to be included in the permit or deny criteria. An IP address in the form ***A.B.C.D***. |
| ***dest-netmask*** | Indication of which bits in the ***dest*** argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the ***dest-wildcard*** argument must be matched by the corresponding bits in the ***dest*** argument. For one-bits in the ***dest-wildcard*** argument the corresponding bits in the ***dest*** argument are ignored. |
| **length** | Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header, regardlessof the specified protocol. |
| ***length*** | Packet length. The range of values is 20 to 65,535. |
| **range** ***length end-length*** | Packets that fall into the range of specified lengths. Each value (***length*** and ***end-length***) can be from 20 to 65,535. |
| **host** ***dest*** | Address of a single-host destination with no wildcarded address bits. The **host** ***dest*** construct is identical to the ***dest dest-wildcard*** construct, if the wildcard address indicates that all bits should be matched (0.0.0.0). |
| **icmp-type** ***icmp-type*** | Optional. Type of Internet Control Message Protocol (ICMP) packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 12. This argument is only available if you specify the ICMP protocol. |
| **icmp-code** ***icmp-code*** | Optional if you use the **icmp-type** ***icmp-type*** construct. A particular ICMP message code to be matched. The range of values is 0 to 255. This argument is only accepted if you specified **icmp** as the ***protocol*** argument. |
| **igmp-type** ***igmp-type*** | Optional. Type of Internet Group Management Protocol (IGMP) packet to be matched. This argument is only accepted if you specified **igmp** as the ***protocol*** argument The range of values is 0 to 15 or one of the keywords listed in Table 13. |
| **dscp eq** ***dscp-value*** | Optional. Packet's Differentiated Services Code Point (DSCP) value must be equal to the value specified in the ***dscp-value*** argument to match the criteria. The range of values is 0 to 63 or one of the keywords listed in Table 14. |
| **established** | Optional. Specifies that only established connections are to be matched. This keyword is only available if you specified **tcp** for the ***protocol*** argument. |

| | |
|---|---|
| `invalid-tcp-flags` | Optional. Specifies that TCP packets with flag combinations other than the following are a match:<br>• SYN<br>• SYN+ACK<br>• ACK<br>• PSH+ACK<br>• URG+ACK<br>• URG+PSH+ACK<br>• FIN<br>• FIN+ACK<br>• RST<br>• RST+ACK<br>Only the lower-order 6 bits (for example, FIN, SYN, RST, PSH, ACK, and URG) in the TCP Flags field are considered for validation. The higher order 6-bits (ECN bits defined by RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, and the reserved bits) are ignored.<br>This keyword is only available if you specify **tcp** for the ***protocol*** argument. |
| `setup` | Optional. Specifies that TCP packets with SYN set and ACK not set in the Flags field are a match.<br>This keyword is only available if you specify **tcp** for the ***protocol*** argument. |
| **precedence** ***prec-value*** | Optional. Precedence value of packets to be considered a match. The range of values is 0 to 7, 7 being the highest precedence, or one of the keywords listed in Table 15. |
| **tos** ***tos-value*** | Optional. Type of service (ToS) to be considered a match. The range of values is 0 to 15 or one of the keywords listed in Table 16. |
| **fragments** | Optional. Allows packet to be permitted or denied based on whether the packet is fragmented. This keyword matches packets where the More-Fragments field is equal to 1 or the IP-Offset field is not equal to 0. |
| **ip-options** | Optional. Specifies that IPv4 packets with the IP Header Length field is greater than 20 are a match. |
| **class** ***class-name*** | Optional. Policy-based class name. Available for policy ACLs only. |
| **condition** ***cond-id*** | Optional. ACL condition ID in integer or IP address format. The ID range of values is 1 to 4,294,967,295. |

## 1.47.4 Default

None

## 1.47.5 Usage Guidelines

Use the **permit** command to create an IP or policy ACL statement to allow packets that meet the specified criteria.

To explicitly set the order of the statement in an ACL, use the **seq permit** command instead of this command.

In IPv4 statements, follow these guidelines:

- The ***cond port*** and ***cond length*** constructs are mutually exclusive with the **range** ***port end-port*** and **range** ***length end-length*** constructs.
- You can use the optional **max-sessions** ***limit*** and **min-sessions** ***limit*** constructs to specify a maximum or minimum number of simultaneous SSH or Telnet sessions allowed from an IP address or subnet. These constructs are available if you use the **service ssh server** or **service telnet server** commands with the **ip access-group** keyword to enable the SSH or Telnet protocol and apply the ACL. For statements where the **any** keyword is specified for both source and destination, only the **max-sessions** ***limit*** construct applies.
- If you specify a limit for both an IP address and the related subnet, the limit for the subnet takes precedence. Similarly, a limit specified for a larger subnet takes precedence over limits specified for related smaller subnets. From all sources combined, the SmartEdge router supports up to 32 active Telnet and SSH sessions.

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

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

Table 8 lists the valid keyword values for the ***protocol*** argument:

*Table 8 Valid Keyword Values for the protocol Argument*

| Keyword | Definition |
|---|---|
| **ahp** | Authentication Header Protocol. |
| **esp** | Encapsulation Security Payload. |
| **gre** | Generic Routing Encapsulation. |
| **icmp** | Internet Control Message Protocol. |
| **igmp** | Internet Group Management Protocol. |
| **ip** | Any IP protocol. |
| **ipinip** | IP-in-IP tunneling. |
| **ospf** | Open Shortest Path First. |
| **pcp** | Payload Compression Protocol. |
| **pim** | Protocol Independent Multicast. |

*Table 8 Valid Keyword Values for the protocol Argument*

| Keyword | Definition |
|---|---|
| `tcp` | Transmission Control Protocol. |
| `udp` | User Datagram Protocol. |

Table 9 lists the valid keyword values for the *`cond`* argument.

*Table 9 Valid Keyword Values for the cond Argument*

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

Table 10 lists the valid keyword values for the `port` argument when it is used to specify a TCP port.

*Table 10   Valid Keyword Values for the port Argument (TCP Port)*

| Keyword | Definition | Corresponding Port Number |
|---|---|---|
| `bgp` | Border Gateway Protocol (BGP) | 179 |
| `chargen` | Character generator | 19 |
| `cmd` | Remote commands (rcmd) | 514 |
| `daytime` | Daytime | 13 |
| `discard` | Discard | 9 |
| `domain` | Domain Name System | 53 |
| `echo` | Echo | 7 |
| `exec` | Exec (rsh) | 512 |
| `finger` | Finger | 79 |
| `ftp` | File Transfer Protocol | 21 |
| `ftp-data` | FTP data connections (used infrequently) | 20 |
| `gopher` | Gopher | 70 |
| `hostname` | Network interface card (NIC) hostname server | 101 |
| `ident` | Identification protocol | 113 |
| `irc` | Internet Relay Chat | 194 |
| `klogin` | Kerberos login | 543 |
| `kshell` | Kerberos Shell | 544 |
| `login` | Login (rlogin) | 513 |
| `lpd` | Printer service | 515 |
| `nntp` | Network News Transport Protocol | 119 |
| `pim-auto-rp` | Protocol Independent Multicast Auto-RP | 496 |
| `pop2` | Post Office Protocol Version 2 | 109 |
| `pop3` | Post Office Protocol Version 3 | 110 |
| `shell` | Remote command shell | 514 |
| `smtp` | Simple Mail Transport Protocol | 25 |
| `ssh` | Secure Shell | 22 |
| `sunrpc` | Sun Remote Procedure Call | 111 |
| `syslog` | System logger | 514 |

*Table 10 Valid Keyword Values for the port Argument (TCP Port)*

| Keyword | Definition | Corresponding Port Number |
|---|---|---|
| `tacacs` | Terminal Access Controller Access Control System | 49 |
| `talk` | Talk | 517 |
| `telnet` | Telnet | 23 |
| `time` | Time | 37 |
| `uucp` | UNIX-to-UNIX Copy Program | 540 |
| `whois` | Nickname | 43 |
| `www` | World Wide Web (HTTP) | 80 |

Table 11 lists the valid keyword values for the *port* argument when it is used to specify a UDP port.

*Table 11 Valid Keyword Values for the port Argument (UDP Port)*

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

Table 12 lists the valid keyword values for the `icmp-type` argument.

*Table 12 Valid Keyword Values for the icmp-type Argument*

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

*Table 12 Valid Keyword Values for the icmp-type Argument*

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

Table 13 lists the valid keyword values for the ***`igmp-type`*** argument.

*Table 13 Valid Keyword Values for the igmp-type Argument*

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

Table 14 lists the valid keyword values for the ***`dscp-value`*** argument.

*Table 14 Valid Keyword Values for the dscp-value Argument*

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

Table 15 lists the valid keyword values for the ***prec-value*** argument.

*Table 15 Valid Keyword Values for the prec-value Argument*

| Keyword | Description |
|---|---|
| `tine` | Specifies routine precedence (value=0). |
| `priority` | Specifies priority precedence (value=1). |
| `immediate` | Specifies immediate precedence (value=2). |
| `flash` | Specifies flash precedence (value=3). |
| `flash-override` | Specifies flash override precedence (value=4). |
| `critical` | Specifies critical precedence (value=5). |
| `internet` | Specifies internetwork control precedence (value=6). |
| `network` | Specifies network control precedence (value=7). |

Table 16 lists the valid keyword values for the ***`tos-value`*** argument.

*Table 16 Valid Keyword Values for the tos-value Argument*

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

## 1.47.6 Examples

The following example specifies that all IP traffic from subnet 10.25/16 is to be allowed. All other traffic is dropped because of the implicit **`deny any any`** statement at the end of the ACL:

```
[local]Redback(config-ctx)#ip access-list protect201
[local]Redback(config-access-list)#permit ip 10.25.0.0 0.0.255.255 any
```

# 1.48 permit (IPv6 ACL)

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

```
permit[protocol] {src-ipv6-addr/prefix-length | any } [cond
] [range port end-port] [dest-ipv6-addr/prefix-length | any
] [icmp-type icmp-type] [icmp-code icmp-code]] [established
| setup | invalid-tcp-flags] [fragments] traffic-class eq
traffic-class-value] [condition cond-id]
```

```
no seq seq-num
```

## 1.48.1 Command Mode

access control list configuration

## 1.48.2 Syntax Descriptions

| | |
|---|---|
| *protocol* | Optional. Number indicating a supported protocol as specified in RFC 1700, *Assigned Numbers*. The range of values is 0 to 255 or one of the keywords listed in:<br>For statements in IPv6 ACLs, see Table 17. |
| *src-ipv6-address/prefix-length*<br>**any** | The traffic source to add to the statement criteria. The *src-ipv6-address* argument is in the format *A:B:C:D::E/prefix-length*, where the prefix length can be from 0 to 128.<br>Indicates that IP traffic to or from all IP addresses is to be included in the **permit** criteria. |
| *cond* | Required if you specify the TCP or UDP protocol. Matching condition according to one of the keywords listed in Table 18. |
| **range** *port end-port* | Optional if you specify the TCP or UDP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must be within the specified range to match the criteria. The range of values is 1 to 65,535 or one of the keywords listed in Table 19 and Table 20. |
| *dest-ipv6-addr/prefix-length* | The traffic destination to be matched. The *src-ipv6-address/prefix-length* argument is in the format *A:B:C:D::E/prefix-length*, where the range of values for the prefix-length can be from 0 to 128. |
| **icmp-type** *icmp-type* | Optional. Type of ICMP packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 21. This argument is only available if you specify **icmp** for the *protocol* argument. |
| **icmp-code** *icmp-code* | Optional if you use the **icmp-type** *icmp-type* construct. A particular ICMP message code to be matched. The range of values is 0 to 255. |
| **established** | Optional with the TCP protocol. Specifies that only established TCP port connections are to be matched. This keyword is only available if you specify **tcp** for the *protocol* argument. |
| **setup** | Optional. Specifies that TCP packets with SYN set and ACK not set in the Flags field are a match.<br>This keyword is only available if you specify **tcp** for the *protocol* argument. |

| | |
|---|---|
| **invalid-tcp-flags** | Optional. Specifies that TCP packets with flag combinations other than the following are a match:<br>• SYN<br>• SYN+ACK<br>• ACK<br>• PSH+ACK<br>• URG+ACK<br>• URG+PSH+ACK<br>• FIN<br>• FIN+ACK<br>• RST<br>• RST+ACK<br>Only the lower-order 6 bits (for example, FIN, SYN, RST, PSH, ACK, and URG) in the TCP Flags field are considered for validation. The higher order 2-bits (ECN bits defined by RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, and the reserved bits) are ignored.<br>This keyword is only available if you specify **tcp** for the ***protocol*** argument.<br>Although you can permit or deny invalid TCP flags, it is recommended you deny it to prevent malicious traffic from entering your network. |
| **traffic eq** ***traffic-class-value*** | Optional. Type of traffic class to be matched. The ***traffic-class-value*** argument is a DSCP; the range of values is from 0 to 63 or one of the DSCP keywords in Table 22. |
| **fragments** | Optional. Allows packet to be permitted or denied based on whether the packet is fragmented. This keyword matches an IPv6 packet, if it has a fragment type extension header.<br>(1) |
| **condition** ***cond-id*** | Optional. Matching ACL condition ID, in integer or IP address format. The ID range of values is 1 to 4,294,967,295. Not supported in IPv6 administrative ACLs applied to the Ethernet management port; conditions are ignored on that port. |

*(1) When defining ACLs with conditions on Layer 4 (L4) parameters such as UDP and TCP ports, keep in mind that only one fragment contains a specific L4 field. In most cases, it will be the first fragment. The ACL is applied to all fragments, and most likely, no matches are made except for the first fragment.*

## 1.48.3 Default

None

## 1.48.4 Usage Guidelines

Use the **permit** command to create an IPv6 access control list (ACL) statement that allows packets that meet the specified criteria.

This command does not set the order of the statement in the ACL; the SmartEdge OS does this automatically. To explicitly set the order of the statements in the ACL, use the *seq* command with the **permit** keyword.

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

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

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

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

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

Table 17 lists the valid keyword values for the ***protocol*** argument:

*Table 17 Valid Keyword Values for the protocol Argument*

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

Table 18 lists the valid keyword values for the ***cond*** argument.

*Table 18 Valid Keyword Values for the cond Argument*

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

Table 19 lists the valid keyword values for the ***port*** argument when it is used to specify a TCP port.

*Table 19 Valid Keyword Values for the port Argument (TCP Port)*

| Keyword | Definition | Corresponding Port Number |
|---|---|---|
| **bgp** | Border Gateway Protocol (BGP) | 179 |
| **chargen** | Character generator | 19 |
| **cmd** | Remote commands (rcmd) | 514 |
| **daytime** | Daytime | 13 |
| **discard** | Discard | 9 |

*Table 19 Valid Keyword Values for the port Argument (TCP Port)*

| Keyword | Definition | Corresponding Port Number |
|---|---|---|
| `domain` | Domain Name System | 53 |
| `echo` | Echo | 7 |
| `exec` | Exec (rsh) | 512 |
| `finger` | Finger | 79 |
| `ftp` | File Transfer Protocol | 21 |
| `ftp-data` | FTP data connections (used infrequently) | 20 |
| `gopher` | Gopher | 70 |
| `hostname` | Network interface card (NIC) hostname server | 101 |
| `ident` | Identification protocol | 113 |
| `irc` | Internet Relay Chat | 194 |
| `klogin` | Kerberos login | 543 |
| `kshell` | Kerberos Shell | 544 |
| `login` | Login (rlogin) | 513 |
| `lpd` | Printer service | 515 |
| `nntp` | Network News Transport Protocol | 119 |
| `pim-auto-rp` | Protocol Independent Multicast Auto-RP | 496 |
| `pop2` | Post Office Protocol Version 2 | 109 |
| `pop3` | Post Office Protocol Version 3 | 110 |
| `shell` | Remote command shell | 514 |
| `smtp` | Simple Mail Transport Protocol | 25 |
| `ssh` | Secure Shell | 22 |
| `sunrpc` | Sun Remote Procedure Call | 111 |
| `syslog` | System logger | 514 |
| `tacacs` | Terminal Access Controller Access Control System | 49 |
| `talk` | Talk | 517 |
| `telnet` | Telnet | 23 |
| `time` | Time | 37 |
| `uucp` | UNIX-to-UNIX Copy Program | 540 |
| `whois` | Nickname | 43 |
| `www` | World Wide Web (HTTP) | 80 |

Table 20 lists the valid keyword values for the `port` argument when it is used to specify a UDP port.

*Table 20 Valid Keyword Values for the port Argument (UDP Port)*

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

Table 21 lists the valid keyword values for the `icmp-type` argument.

*Table 21 Valid Keyword Values for the icmp-type Argument*

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

Table 22 lists the valid keyword values for the `traffic-class-value` argument.

*Table 22 Valid Keyword Values for the traffic-class-value (DSCP) Argument*

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

### 1.48.5 Examples

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

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

# 1.49 {permit | deny}

```
{permit | deny} {reg-exp | any} | {community-num | ext-community-num
| local-as | no-advertise | no-export | any | reg-exp reg-exp} |
{{ip-addr/prefix-length | ipv6-addr/prefix-length} [{eq eq-value | ge
ge-value | [le le-value]}] | any}:
```

```
seq seq-num {permit | deny} {reg-exp | any} | {community-num |
ext-community-num | local-as | no-advertise | no-export | any |
reg-exp reg-exp} | {ip-addr/prefix-length [{eq eq-value | ge ge-value
| [le le-value]}] | any}
```

```
no seq seq-num
```

## 1.49.1 Purpose

Permits or denies routes matching the specified criteria.

## 1.49.2 Command Mode

- AS path list configuration
- community list configuration
- extended community list configuration
- IP prefix list configuration
- IPv6 prefix list configuration

### 1.49.3 Syntax Description

AS path list configuration mode:

| | |
|---|---|
| *reg-exp* | AS path regular expression. |
| **any** | Wildcard that matches on any AS path list number. |
| *community-num* | Community number, which can be specified only when configuring a community list. It can be expressed in either of the following formats:<br>• ***asn*:*nn***, where ***asn*** is the autonomous system number (ASN) and ***nn*** is a 16-bit integer. The range of ***nn*** values is 0 to 65,535.<br>• An unsigned decimal value. The range of values is 1 to 4,294,967,040.<br>You can specify a single community number or multiple community numbers separated by a space. (All numbers must match a community in the route being tested in order for the statement to match.) |
| *ext-community-num* | Extended community number, which can be specified only when configuring an extended community list. It can be expressed in either of the following formats:<br>• ***tt*:*asn*:*nnnn***, where ***tt*** is the extended community type, ***asn*** is the ASN, and ***nnnn*** is either a 32-bit integer or a 16-bit integer, depending on the size of the ASN. The extended community type identifies either a target or origin community. The target community identifies the destination to which the route is going, and the origin community identifies source from where the route originated. The ***tt*** argument is a placeholder for either the **ro** (route origin) keyword, or the **rt** (route target) keyword. You can specify the ASN as either a two-byte (two-octet) or four-byte (four-octet) integer. A value of 65535 or lower is interpreted as a two-byte integer, unless you add an **L** suffix (for example, **125L**), in which case it is interpreted as a four-byte integer. A value larger than 65535 is always interpreted as a four-byte integer, and the **L** suffix is optional. If the ASN is two-bytes, then ***nnnn*** is a 32-bit integer. If the ASN is four-bytes, then ***nnnn*** is a 16-bit integer.<br>• ***tt*:*ip-addr*:*nn***, where ***tt*** is the extended community type, ***ip-addr*** is the IP address in the form ***A*.*B*.*C*.*D***, and ***nn*** is a 16-bit integer.<br>You can specify a single extended community number or multiple extended community numbers separated by a space. (All numbers must match an extended community in the route being tested in order for the statement to match.) |
| **local-as** | Propagates this route to peers in other subautonomous systems within the confederation. Does not advertise this route to an external Border Gateway Protocol (eBGP) peer. |
| **no-advertise** | Does not advertise this route to any peer (internal or external). |
| **no-export** | Does not advertise this route out of the confederation, or out of the local AS, if this peer is not part of a confederation. |
| **reg-exp** *reg-exp* | Regular expression used to match the ASCII representation of the route's community attribute. The ASCII representation of the community attributes includes all the communities in ***aa*:*nn*** format. Each entry must be separated by a space. |
| **any** | Wildcard that matches on any community number. |

IP prefix list configuration mode:

| | |
|---|---|
| *ip-addr* | IP address in the form *A.B.C.D*. |
| *prefix-length* | Prefix length. The range of values is 0 to 32. |
| eq *eq-value* | Optional. Equal to value. The *eq-value* argument specifies a value to which a route's prefix length must match; the eq keyword indicates that the route's prefix length must exactly match the *eq-value*. The range of values for the *eq-value* argument is 1 to 32. |
| ge *ge-value* | Optional. Greater than or equal to value. The *ge-value* argument specifies a value to which a route's prefix length must match; the ge keyword indicates that the route's prefix length must be greater than or equal to the *ge-value* to match. The range of values for the *ge-value* argument is 1 to 32. |
| le *le-value* | Optional. Less than or equal to value. The *le-value* argument specifies a value to which a route's prefix length must match; the le keyword indicates that the route's prefix length must be less than or equal to the le-value to match. The range of values for the *le-value* argument is 1 to 32. |
| any | Wildcard that matches on any prefix. |

IPv6 prefix list configuration mode:

| | |
|---|---|
| *ipv6-addr* | IP Version 6 (IPv6) address in the form *A*:*B*:*C*:*D*:*E*:*F*:*G*:*H*. |
| **prefix-length** | Prefix length. The range of values is 0 to 128. |
| eq *eq-value* | Optional. Equal to value. The *eq-value* argument specifies a value to which a route's prefix length must match; the **eq** keyword indicates that the route's prefix length must exactly match the *eq-value*. The range of values for the *eq-value* argument is 1 to 128. |
| ge *ge-value* | Optional. Greater than or equal to value. The *ge-value* argument specifies a value to which a route's prefix length must match; the **ge** keyword indicates that the route's prefix length must be greater than or equal to the *ge-value* to match. The range of values for the *ge-value* argument is 1 to 128. |
| le *le-value* | Optional. Less than or equal to value. The *le-value* argument specifies a value to which a route's prefix length must match; the **le** keyword indicates that the route's prefix length must be less than or equal to the le-value to match. The range of values for the *le-value* argument is 1 to 128. |
| **any** | Wildcard that matches on any prefix. |

## 1.49.4 Default

None

## 1.49.5 Usage Guidelines

Use the {**permit** | **deny**} command to permit or deny any routes matching the specified criteria.

Use the **seq** *seq-num* form of this command to specify the sequence number of the statement you are creating. If you do not use the **seq** *seq-num* construct, the system automatically assigns sequence numbers in increments of 10. The range of values is 1 to 4,294,967,295.

Use the **no seq** *seq-num* form of this command to delete a specific sequence number from the AS path list, community list, extended community list, IP prefix list, or IPv6 prefix list.

**Note:** A high prefix length value specifies a small subnet, and a low prefix length value specifies a large subnet. Using the **ge** keyword permits or denies routes with higher prefix length values (smaller subnets), and the **le** keyword permits or denies routes with lower prefix length values (larger subnets).

If you are using an extended community number in a regular expression, you can use the **L** suffix as part of the ASN definition.

### 1.49.6 Examples

The following example ensures that the BGP neighbor at IP address **10.1.1.1** is not sent advertisements about any path to or from the adjacent autonomous system **3:**

```
[local]Redback(config-ctx)#as-path-list aspath-1
[local]Redback(config-as-path-list)#seq 5 deny _3_
[local]Redback(config-ctx)#as-path-list 10 seq 10 permit .*
[local]Redback(config-ctx)#route-map drop-asp-3 permit 10
[local]Redback(config-route-map)#match as-path-list 10
.
.
.
[local]Redback(config-ctx)#router bgp 65015
[local]Redback(config-group)#neighbor 10.1.1.1
[local]Redback(config-peer)#route-map drop-asp-3 out
```

The following example configures community list **permit_local** to propagate routes to peers within the local autonomous system (**local-AS**):

```
[local]Redback(config-ctx)#community-list permit_local
[local]Redback(config-community-list)#seq 10
[local]Redback(config-community-list)#permit local-AS
```

## 1.50 pim accept-rp

**pim accept-rp** ***rp-addr*** [***acl-name***]

**no pim accept-rp** ***rp-addr***

### 1.50.1 Purpose

Accepts an IP address as being a valid rendezvous point (RP) address for a specific Internet Group Management Protocol (IGMP) group.

### 1.50.2 Command Mode

context configuration

### 1.50.3 Syntax Description

| | |
|---|---|
| ***rp-addr*** | IP address of the RP. |
| ***acl-name*** | Optional. Name of the access control list (ACL) used to filter RP addresses. |

### 1.50.4 Default

None

### 1.50.5 Usage Guidelines

Use the **pim accept-rp** command to accept an IP address as being a valid RP address for a specific IGMP group.

To determine if the RP should be accepted, the router checks the Group-to-RP mapping cache for a matching entry for the group. If there is a matching entry, the RP is accepted.

Use the ***acl-name*** argument to compare the RP address to the specified ACL to determine if the filter permits the RP address.

Use the **no** form of this command to remove an accepted RP address.

### 1.50.6 Examples

The following example configures the router to accept or reject the RP address, **192.168.100.1**, as a valid RP:

```
[local]Redback(config)#context isp1
[local]Redback(config-ctx)#pim accept-rp 192.168.100.1
```

# 1.51 pim anycast-rp

**`pim anycast-rp`** *`anycast-addr rp-addr`*

**`no pim anycast-rp`** *`anycast-addr rp-addr`*

## 1.51.1 Purpose

Configures anycast rendezvous point (RP) functionality on a Protocol Independent Multicast-Sparse Mode (PIM-SM) router.

## 1.51.2 Command Mode

context configuration

## 1.51.3 Syntax Description

| | |
|---|---|
| *`anycast-addr`* | IP address of the anycast RP set. This is the IP address used by the multicast groups or sources to join or register. |
| *`rp-addr`* | IP address of the router configured with anycast RP. This is the IP address to where the Register messages are forwarded. |

## 1.51.4 Default

Anycast RP is not configured on the router.

## 1.51.5 Usage Guidelines

Use the **`pim anycast-rp`** command to configure anycast RP functionality on a PIM-SM router.

**Note:** This command must be configured for each router that belongs to the same anycast RP set in the domain.

Use the **`no`** form of this command to disable anycast RP functionality on a PIM-SM router.

## 1.51.6 Examples

The following example configures the IP address for the anycast RP to **10.10.10.20**, and the IP address of the router to **192.168.20.34:**

```
[local]Redback(config-ctx)#pim anycast-rp 10.10.10.20 192.160.20.34
```

## 1.52 pim bfd

**pim bfd**

{**no** | **default**} **pim bfd**

### 1.52.1 Purpose

Enables BFD for a PIM interface that has BFD disabled.

### 1.52.2 Command Mode

interface configuration.

### 1.52.3 Syntax Description

This command has no keywords or arguments.

### 1.52.4 Default

BFD is automatically enabled on an interface when PIM is enabled on that interface.

### 1.52.5 Usage Guidelines

Use the **pim bfd** command to enable BFD on a PIM interface that has BFD disabled. PIM interfaces that have BFD disabled do not receive BFD status updates from neighbors.

**Note:** BFD is automatically enabled on an interface when PIM is enabled on that interface. You must use the **no pim bfd** command to disable BFD on a PIM interface.

Use the **show pim interface** command to see if BFD is enabled or disabled on an interface.

Use the **no** form of this command to disable BFD on a PIM interface. Use the **default** form of this command to reenable BFD on a PIM interface that has BFD disabled.

### 1.52.6 Examples

The following example shows how to disable BFD on a PIM interface:

```
[local]Redback(config-ctx)#interface foo
[local]Redback(config-if)#no pim bfd
```

The following example shows how to reenable BFD on a PIM interface that has BFD disabled:

```
[local]Redback(config-ctx)#interface foo
[local]Redback(config-if)#pim bfd
```

# 1.53 pim bsr-border

**pim bsr-border**

**no pim bsr-border**

## 1.53.1 Purpose

Configures the router to neither send nor receive bootstrap router (BSR) messages.

## 1.53.2 Command Mode

interface configuration

## 1.53.3 Syntax Description

This command has no keywords or arguments.

## 1.53.4 Default

None

## 1.53.5 Usage Guidelines

Use the **pim bsr-border** command to configure the router to neither send nor receive BSR messages.

**Note:** This command should be configured on routers that connect to bordering Protocol Independent Multicast (PIM) domains to create a PIM domain boundary that blocks the flow of PIM Version 2 (PIMv2) BSR messages across the domain border.

Use the **no** form of this command to resume the flow of BSR messages to and from the router.

### 1.53.6 Examples

The following example configures the router to neither send nor receive BSR messages:

```
[local]Redback(config-ctx)#interface enet01
[local]Redback(config-if)#pim bsr-border
```

# 1.54 pim bsr-candidate

**pim bsr-candidate** ***if-name hash-mask-len priority***

**no pim bsr-candidate** ***if-name hash-mask-len priority***

## 1.54.1 Purpose

Configures a router to begin serving as a candidate bootstrap router (C-BSR).

## 1.54.2 Command Mode

context configuration

## 1.54.3 Syntax Description

| | |
|---|---|
| ***if-name*** | Unicast rendezvous point (RP) address corresponding to the IP address of the interface to be used by the BSR. |
| ***hash-mask-len*** | Value contained in BSR messages that will be used by all routers to hash (map) to an RP. It is recommended to use a value between 24 and 30. |
| ***priority*** | Value used to specify the BSR election priority among different candidate BSRs. A larger value wins over a smaller value. |

## 1.54.4 Default

None

## 1.54.5 Usage Guidelines

Use the **pim bsr-candidate** command to configure a router to begin serving as a C-BSR. and participate in the BSR election process. If this router wins the BSR election, all candidate RPs advertise their candidacy to this router. The BSR caches and advertises the RP sets via the Protocol Independent Multicast (PIM) bootstrap messages to the entire PIM domain.

Use the **no** form of this command to decline the router’s BSR candidacy.

## 1.54.6 Examples

The following example configures a router to begin serving as a C-BSR using the interface, **intfe1/1**, with a hash mask length of **27** and a priority of **12:**

```
[local]Redback(config)#context isp01
[local]Redback(config-ctx)#pim bsr-candidate intfe1/1 27 12
```

# 1.55 pim dense-mode

**`pim dense-mode`**

{**`no`** | **`default`**} **`pim dense-mode`**

## 1.55.1 Purpose

Enables Protocol Independent Multicast-Dense Mode (PIM-DM).

## 1.55.2 Command Mode

interface configuration

## 1.55.3 Syntax Description

This command has no keywords or arguments.

## 1.55.4 Default

None

## 1.55.5 Usage Guidelines

Use the **`pim dense-mode`** command to enable PIM-DM on an interface.

Use the **`no`** or **`default`** form of this command to disable PIM-DM on an interface.

## 1.55.6 Examples

The following example enables PIM-DM on the interface, **southpoint:**

```
[local]Redback(config-ctx)#interface southpoint
[local]Redback(config-if)#pim dense-mode
```

# 1.56 pim dr-priority

**pim dr-priority** ***priority***

{**no** | **default**} **pim dr-priority** ***priority***

## 1.56.1 Purpose

Specifies the election priority value for a designated router (DR).

## 1.56.2 Command Mode

interface configuration

## 1.56.3 Syntax Description

| | |
|---|---|
| ***priority*** | Value used in the DR election process. The router with the highest priority value is elected as the DR. |

## 1.56.4 Default

The default priority value is 1.

## 1.56.5 Usage Guidelines

Use the **pim dr-priority** command to specify the election priority value for a DR.

Use the **no** or **default** form of this command to set the election priority to the default value of 1.

## 1.56.6 Examples

The following example sets the election priority value to **3:**

```
[local]Redback(config-ctx)#interface enet1
[local]Redback(config-if)#pim dr-priority 3
```

# 1.57 pim dual-join

**pim dual-join group** ***ip_addr*** **source** ***ip_addr***

**no pim dual-join group** ***ip_addr*** **source** ***ip_addr***

## 1.57.1 Purpose

Enables pim-dual configuration mode

## 1.57.2 Command Mode

context configuration

## 1.57.3 Syntax Description

| | |
|---|---|
| **group** ***ip_addr*** | Specifies the IP address of the multicast group of the current PIM-Dual join session. The range of addresses is 224.0.0.0 to 239.255.255.255. |
| **source*****ip_addr*** | Specifies the unicast IP address of multicast server for the current PIM-Dual join session. The range of addresses is 224.0.0.0 to 239.255.255.255. |

## 1.57.4 Default

None

## 1.57.5 Usage Guidelines

Use the **pim dual-join** command to enable pim-dual configuration mode.

Use the **no** form of this command to disable pim-dual configuration mode.

## 1.57.6 Examples

The following example show how to enable pim-dual join mode on the **local** context and create a group with an IP address of **225.100.1.1:**

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

# 1.58 pim graceful-restart

```
pim graceful-restart

no pim graceful-restart

default fault pim graceful-restart
```

## 1.58.1 Purpose

Enables Protocol Independent Multicast (PIM) graceful restart on the specified context.

## 1.58.2 Command Mode

context configuration

## 1.58.3 Syntax Description

This command has no keywords or arguments.

## 1.58.4 Default

PIM graceful restart is enabled.

## 1.58.5 Usage Guidelines

Use the **`pim graceful-restart`** command to enable PIM graceful restart on the specified context. PIM graceful restart allows the SmartEdge router and its neighbors to continue forwarding multicast packets without disrupting network traffic. Because neighboring routers assist, the SmartEdge router can quickly restart the PIM process without having to recalculate algorithms from scratch.

A generation ID (GenID), used in Hello messages, is generated randomly when the PIM process initially starts, or restarts after a crash. PIM uses the GenID to establish neighbor relationships with other PIM routers in the network. All neighbors that support graceful restart acknowledge the new GenID by sending multicast updates to the restarting neighbor.

The SmartEdge router stores the GenID of every PIM neighbor, and when it detects a new GenID for a neighbor, it performs one of the following functions:

- If the neighbor restarts more than five times within its hello interval hold time, which is 105 seconds by default, PIM defers its neighbor recovery mechanism and generates the following INFO message:**Nbr restarted 6 times (> 5) within 105 secs, backoff nbr recovery**

- If a candidate RP neighbor restarts, PIM sends a candidate RP advertisement to the bootstrap router (BSR).

- If a reverse path forwarding (RPF) neighbor (which is an assert winner) restarts, PIM clears its RPF assert winner information and the RPF reverts back to the original RPF (pointed by unicast routing).

If PIM graceful restart is enabled, the **`show configuration pim verbose`** command displays **pim graceful restart** in the configuration; however, if it is disabled, the **`show configuration pim`** command (non-verbose) displays **no pim graceful restart** in the configuration. For more information about the **`show configuration pim`** and **`show configuration pim verbose`** commands, see *Configuring IP Multicast*.

Use the **`no`** form of this command to disable PIM graceful restart.

Use the **`default`** form of this command to return to the default PIM graceful restart state, which is enabled.

### 1.58.6 Examples

The following example enables PIM graceful restart on the context, **foo**, where PIM graceful restart had been previously disabled:

```
[local]Redback(config)#context foo
[local]Redback(config-ctx)#pim graceful-restart
```

# 1.59 pim hello-interval

**pim hello-interval** ***interval***

{**no** | **default**} **pim hello-interval** ***interval***

## 1.59.1 Purpose

Sets the Protocol Independent Multicast Version 2 (PIMv2) Hello interval.

## 1.59.2 Command Mode

interface configuration

## 1.59.3 Syntax Description

| | |
|---|---|
| *interval* | Interval, in seconds, at which PIMv2 Hello messages are sent. Range is from 10 to 1800 seconds; the default interval is 30 seconds. |

## 1.59.4 Default

The default PIM Hello interval is 30 seconds.

## 1.59.5 Usage Guidelines

Use the **pim hello-interval** command to set the PIMv2 Hello interval.

Use the **no** or **default** form of this command to set the Hello interval to the default value.

## 1.59.6 Examples

The following example sets the PIM Hello interval to **65** seconds:

```
[local]Redback(config-ctx)#interface enet1
[local]Redback(config-if)#pim hello-interval 65
```

## 1.60 pim neighbor-filter

**pim neighbor-filter** ***acl-name***

**no pim neighbor-filter**

### 1.60.1 Purpose

Filters Protocol Independent Multicast (PIM) messages from neighbors.

### 1.60.2 Command Mode

interface configuration

### 1.60.3 Syntax Description

| | |
|---|---|
| *acl-name* | Name of the access control list (ACL) used to filter PIM messages from neighbors. |

### 1.60.4 Default

None

### 1.60.5 Usage Guidelines

Use the **pim neighbor-filter** command to filter PIM messages from neighbors. PIM messages are accepted only if the neighbor's IP address is permitted by the ACL.

Use the **no** form of this command to accept all PIM messages from neighbors.

### 1.60.6 Examples

The following example filters PIM messages from neighbors using the **Neighbors44** ACL:

```
[local]Redback(config-ctx)#interface enet1
[local]Redback(config-if)#pim neighbor-filter Neighbors44
```

# 1.61 pim operation-mode

**pim operation-mode** {**standard** | **legacy**}

## 1.61.1 Purpose

Sets the protocol parameters to be compatible with Protocol Independent Multicast Sparse-Mode (PIM-SM) specifications, or to be compatible with legacy implementations.

## 1.61.2 Command Mode

context configuration

## 1.61.3 Syntax Description

| | |
|---|---|
| `standard` | Configures compatibility with PIM-SM specifications. |
| `legacy` | Configures compatibility with legacy implementations. |

## 1.61.4 Default

The protocol parameters are compatible with legacy implementations.

## 1.61.5 Usage Guidelines

Use the **pim operation-mode** command to set the protocol parameters to be compatible with PIM-SM specifications, or to be compatible with legacy implementations, such as traditional Cisco implementations.

### 1.61.6 Examples

The following example sets the protocol parameters to be compatible with PIM-SM specifications:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#pim operation-mode standard
```

# 1.62 pim rp-address

**`pim rp-address`** *`rp-addr`* [*`acl-name`*]

**`no pim rp-address`** *`rp-addr`*

## 1.62.1 Purpose

Configures a router with the rendezvous point (RP) address.

## 1.62.2 Command Mode

context configuration

## 1.62.3 Syntax Description

| | |
|---|---|
| *`rp-addr`* | IP address of the RP. |
| *`acl-name`* | Optional. Name of the access control list (ACL) used to filter multicast groups using the RP. |

## 1.62.4 Default

None

## 1.62.5 Usage Guidelines

Use the **`pim rp-address`** command to configure a router with the RP address for all Internet Group Management Protocol (IGMP) group addresses permitted by an ACL. If an ACL is not specified, this RP address is used for the entire multicast address space.

The **`pim rp-address`** command is generally used on simple Protocol Independent Multicast sparse mode (PIM-SM) networks where the RP address is manually configured on each router in the network. More complicated networks should use the PIM Version 2 (PIMv2) bootstrap router (BSR) feature, which allows routers on a network to dynamically learn the RP address.

Use the **`no`** form of this command to remove the RP address from the router.

### 1.62.6 Examples

The following example configures a router with the RP address of **192.168.200.20:**

```
[local]Redback(config)#context isp1
[local]Redback(config-ctx)#pim rp-address 192.168.200.20
```

# 1.63 pim rp-candidate

**pim rp-candidate** ***if-name*** [**group-list** ***acl-name***]

**no pim rp-candidate** ***if-name***

## 1.63.1 Purpose

Configures a candidate rendezvous point (C-RP) on an interface.

## 1.63.2 Command Mode

context configuration

## 1.63.3 Syntax Description

| | |
|---|---|
| ***if-name*** | Name of the interface to be used by the C-RP. |
| **group-list** ***acl-name*** | Optional. Name of the access control list (ACL) used to filter Internet Group Management Protocol (IGMP) group IP addresses. |

## 1.63.4 Default

None

## 1.63.5 Usage Guidelines

Use the **pim rp-candidate** command to configure a C-RP on an interface for group address ranges permitted by an ACL. If an ACL is not specified, this RP address is used for the entire multicast address space.

Use the **no** form of this command to decline the C-RP's candidacy from the interface.

## 1.63.6 Examples

The following example configures a C-RP on the interface, **loopback22:**

```
[local]Redback(config)#context isp1
[local]Redback(config-ctx)#pim rp-candidate loopback22
```

## 1.64 pim sparse-mode

**pim sparse-mode** [**passive**]

**no pim sparse-mode** [**passive**]

### 1.64.1 Purpose

Enables Protocol Independent Multicast Sparse-Mode (PIM-SM).

### 1.64.2 Command Mode

interface configuration

### 1.64.3 Syntax Description

| | |
|---|---|
| `passive` | Optional. Specifies that no PIM messages are exchanged out of the interface, but the interface, or circuits belonging to the interface, can be populated in a multicast forwarding entry by receiving an Internet Group Management Protocol (IGMP) report or a data packet. |

### 1.64.4 Default

None

### 1.64.5 Usage Guidelines

Use the **pim sparse-mode** command to enable PIM-SM on an interface.

PIM-SM is not supported on multibind interfaces. If you are configuring a multibind interface, you must use the **pim sparse-mode passive** command in interface configuration mode to prevent PIM messages from being exchanged on the egress interface, while allowing the interface and its circuits to be populated in a multicast forwarding entry by receiving an IGMP report or a data packet.

Consider the following restrictions when configuring multicast for subscribers:

- If the multicast source uses a router-mode CPE, the SmartEdge router runs in active PIM-SM only.

- If the multicast receiver uses a router-mode CPE, the SmartEdge router runs in active PIM-SM or passive PIM-SM.

- If a bridge-mode CPE exists between the multicast source or receiver and the SmartEdge router, the SmartEdge router can run in active PIM-SM or passive PIM-SM.

Use the **no** form of this command to disable PIM-SM on an interface.

### 1.64.6 Examples

The following example enables PIM-SM on the interface, **Northpoint:**

```
[local]Redback(config-ctx)#interface Northpoint
[local]Redback(config-if)#pim sparse-mode
```

# 1.65 pim spt-threshold infinity

**pim spt-threshold infinity** [**group-list** *acl*]

**no pim spt-threshold infinity** [**group-list** *acl*]

## 1.65.1 Purpose

Enables a Protocol Independent Multicast-Sparse Mode (PIM-SM) leaf router to continue using a shared tree, instead of switching to a shortest-path tree (SPT).

## 1.65.2 Command Mode

context configuration

## 1.65.3 Syntax Description

| | |
|---|---|
| **group-list** *acl* | Optional. Groups permitted by the access control list (ACL) to stay on the shared tree. If the **group-list** *acl* construct is not used, or if the *acl* value is 0, the threshold applies to all groups. |

## 1.65.4 Default

The SPT threshold is set to 0, and the switchover occurs immediately after the initial transmission has been established.

## 1.65.5 Usage Guidelines

Use the **pim spt-threshold infinity** command to enable a PIM-SM leaf router to continue using a shared tree, instead of switching to an SPT.

A multicast source initially sends traffic using the shared tree; however, after transmitting a certain number of bits (the SPT threshold), the PIM-SM router switches from using the shared tree to using the SPT. Using the **pim spt-threshold infinity** command sets the SPT threshold infinitely high, making it impossible for the switchover to occur.

Use the **no** form of this command to allow a PIM-SM leaf router to switch from a shared tree to an SPT.

### 1.65.6 Examples

The following example enables a PIM-SM leaf router to continue using a shared tree:

```
[local]Redback(config-ctx)#pim spt-threshold infinity
```

# 1.66 pim ssm

**pim ssm** {**default** | **range** ***acl-name***}

**no pim ssm** {**default** | **range** ***acl-name***}

## 1.66.1 Purpose

Enables source-specific multicast (SSM) routing on the specified context and sets the range of addresses to be used for SSM.

## 1.66.2 Command Mode

context configuration

## 1.66.3 Syntax Description

| | |
|---|---|
| `default` | Uses the default SSM address range, which is 232.0.0.0/8. |
| `range` *`acl-name`* | Uses the specified access control list (ACL) to define the SSM address range. |

## 1.66.4 Default

SSM routing is not enabled.

## 1.66.5 Usage Guidelines

Use the **pim ssm** command to enable SSM routing on the specified context.

The SSM feature is an extension of multicast routing where traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured to use SSM, only source-specific multicast distribution trees (MDTs) are created, and not shared trees.

Protocol Independent Multicast-SSM (PIM-SSM) is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). SSM is supported by the Internet Group Management Protocol Version 3 (IGMPv3).

The address range 232.0.0.0 to 232.255.255.255 is reserved for SSM applications and protocols. Existing IP multicast receivers cannot receive traffic when trying to use addresses in a defined SSM range, unless they are SSM enabled.

The SmartEdge OS supports using the default SSM address range of 232.0.0.0/8; alternatively, you can define your own address range in an ACL and apply the ACL using the **range** keyword. For information about configuring ACLs, see *Configuring ACLs*.

For more information on SSM routing, see the Internet Draft, *Source-Specific Multicast for IP*, *draft-ietf-ssm-arch-00.txt*.

Use the **no** form of this command to disable SSM routing on an interface.

### 1.66.6 Examples

The following example enables SSM routing on the **local** context using the default address range (232.0.0.0/8):

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#pim ssm default
```

# 1.67 pim state-refresh origination-interval

**`pim state-refresh origination-interval`** [*`interval`*]

{**`no`** | **`default`**} **`pim state-refresh origination-interval`** [*`interval`*]

## 1.67.1 Purpose

Enables the origination (sending) of Protocol Independent Multicast-Dense Mode (PIM-DM) State Refresh control messages.

## 1.67.2 Command Mode

interface configuration

## 1.67.3 Syntax Description

| | |
|---|---|
| *`interval`* | Optional. Interval between PIM-DM State Refresh control messages. The range of values, in seconds, is 4 to 100; the default value is 60. |

## 1.67.4 Default

The origination of PIM-DM State Refresh messages is disabled.

## 1.67.5 Usage Guidelines

Use the **`pim state-refresh origination-interval`** command to enable the origination of PIM-DM State Refresh control messages.

The PIM-DM State Refresh feature keeps pruned branches from being automatically restored to the PIM-DM network by periodically forwarding control messages down the broadcast tree. The control messages refresh the prune state on the outgoing interfaces of each router in the broadcast tree. Enabling this feature is useful in situations in which restoring previously pruned branches consumes too much bandwidth by reflooding unwanted traffic over the PIM-DM network.

Use the **`no`** or **`default`** form of this command to disable the origination of the PIM-DM State Refresh control messages.

### 1.67.6 Examples

The following example enables the origination of PIM-DM State Refresh control messages and configures an interval of **60** seconds between control messages:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface foo
[local]Redback(config-if)#pim state-refresh origination-interval 60
```

# 1.68 pim static group

**pim static group** *group-addr* [**oif** *if-name* | **source** *ip-addr* [**oif** *if-name* | **register** | **send-join**]]

**no pim static group** *group-addr* [**oif** *if-name* | **source** *ip-addr* [**oif** *if-name* | **register** | **send-join**]]

## 1.68.1 Purpose

Creates a static multicast route, (*,G) or (S,G), with the specified interface as the outgoing interface (OIF).

## 1.68.2 Command Mode

context configuration

## 1.68.3 Syntax Description

| | |
|---|---|
| *group-addr* | Multicast group IP address. |
| oif *if-name* | Optional. OIF name. |
| register | Optional. Enables the first-hop router to send register messages to the rendezvous point (RP). |
| source *ip-addr* | Optional. Multicast source IP address. |
| send-join | Optional. Sends a join message to the reverse path forwarding (RPF) neighbor. |

## 1.68.4 Default

No static multicast routes are created.

## 1.68.5 Usage Guidelines

Use the **pim static group** command to create a static multicast route, (*,G) or (S,G), with the specified interface as the OIF.

**Note:** Protocol Independent Multicast (PIM) normally creates dynamic multicast routes; the **pim static group** command allows you to create static multicast routes.

An OIF is an outgoing circuit that receives traffic destined for a given multicast group. For this command, the OIF is a regular interface. For multibind interface OIFs, configure the **static-group** command in an Internet Group Management Protocol (IGMP) service profile that is bound to a subscriber (default) profile.

Use the **register** keyword to configure multicast static groups on the first-hop router, which is the router directly connected to the multicast source, so that this router can send register messages to the RP.

Use the **no** form of this command to delete the static multicast route.

### 1.68.6 Examples

The following example creates a static multicast route, **224.1.1.1**, with **fxp1** as its OIF:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#pim static group 224.1.1.1 oif fxp1
```

# 1.69 ping

**ping** {*ip-addr*} [*number-of-packets*] [**df**] [**flood**] [**numeric**] [**pattern** *hex-pattern*] [**preload**] [**quiet**] [**record**] [**silent**] [**size** *bytes*] [**source** *ip-addr*] [**timeout** *seconds*] [**tos**] [**ttl**] [**verbose**]

## 1.69.1 Purpose

Tests whether the host is reachable.

## 1.69.2 Command Mode

- exec

## 1.69.3 Syntax Description

| | |
|---|---|
| *ip-addr* | IP address of the host. |
| *number-of-packets* | Optional. Number of ping packets to send. The range of values is 1 to 2,147,483,647; the default value is 5. |
| **df** | Optional. Indicates that the packet should not be fragmented in the IP header. |
| **flood** | Optional. Floods ping packets. |
| **numeric** | Optional. Specifies numeric output only. |
| **pattern** *hex-pattern* | Optional. Hexadecimal pattern to fill in Internet Control Message Protocol (ICMP) packets. The range of values is 0x0 to 0xffff. |
| **preload** | Optional. Sends packets as quickly as possible. |
| **quiet** | Optional. Suppresses ICMP error messages. |
| **record** | Optional. Specifies that the RECORD_ROUTE option is to be included in the ECHO_REQUEST packet. |
| **silent** | Optional. Displays only summary lines at start up. |
| **size** *bytes* | Optional. Size, in bytes, of the IP datagram. The range of values is 10 to 2,000; the default value is 36. |
| **source** *ip-addr* | Optional. Source IP address. |
| **timeout** *seconds* | Optional. Interval, in seconds, that the system waits for a response for each ping packet. The range of values is 1 to 120; the default value is 1. |
| **tos** | Optional. Specifies the type of service (ToS) in hexadecimal. The range of values is 0x0 to 0xff; the default value is 0. |
| **ttl** | Optional. Specifies the time-to-live (TTL) value. The range of values is 1 to 255; the default value is 255. |
| **verbose** | Optional. Enables all possible output. |

## 1.69.4 Default

Sends 56-byte packets to the specified host, using a timeout value of one second.

### 1.69.5 Usage Guidelines

Use the **ping** command (in exec mode) to test whether the host is reachable.

Press **Ctrl+C** to stop a ping test.

You can only use the ***hostname*** argument if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands (in context configuration mode). For more information about these commands, see *Configuring DNS*.

The **ping** and **traceroute** commands (in exec mode) can have vastly different output, depending on the context in which the commands are issued. In particular, an IP address that can be reached by the **ping** or **traceroute** command in one context might not be reachable from another context. Use the **context** command (in exec mode) to switch between contexts.

**Note:** The source address must be specified when pinging an IPv6 address on the provider edge (6PE) across the Multiprotocol Label Switching (MPLS) backbone.

Use the **ping atm** command (in exec mode) to test Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) by sending operations, administration, and maintenance (OAM) loopback cells. This command tests the reachability of a neighboring ATM switch or the end of an ATM connection.

The SmartEdge router does not allow multiple administrators to ping the same ATM PVC at the same time. If one administrator has issued the **ping** command on an ATM PVC, no other administrators can do so until the first is finished.

Use the **ping ancp** command (in exec mode) to test digital subscriber line (DSL) circuits by sending a port management message to the ANCP neighbor peer to test the peer.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

Table 23 lists the characters for the ICMP errors that can be displayed in the output and the error descriptions.

*Table 23 ICMP Error and Message Code Descriptions*

| Character | ICMP Error and Message Code Description |
|---|---|
| ! | No error |
| ? | Unknown error code |
| a | Host access prohibited |
| A | Network access prohibited |
| c | Precedence cutoff |
| C | Communication prohibited |

*Table 23 ICMP Error and Message Code Descriptions*

| Character | ICMP Error and Message Code Description |
|---|---|
| d | Router solicitation |
| D | Router Advertisement |
| F | Unreachable because packet requires fragmentation, but “Don’t Fragment” bit is set |
| F | Time-to-live exceeded in reassembly |
| h | Host isolated |
| H | Host unknown |
| i | Information reply |
| I | Information request |
| L | Time-to-live exceeded in transmission |
| m | Timestamp reply |
| M | Timestamp |
| n | Network unknown |
| N | Network unreachable |
| p | Port unreachable |
| P | Protocol unreachable |
| Q | Packet lost due to traffic congestion |
| r | Redirected by host |
| R | Redirected by network |
| S | Unreachable because source route failed |
| t | Bad ToS for host |
| t | Redirected by host because of ToS |
| T | Bad ToS for network |
| T | Redirected by network because of ToS |
| U | Host unreachable |
| V | Host precedence violation |
| x | Address mask reply |
| X | Address mask request |
| Z | ICMP parameter problem |

### 1.69.6 Examples

The following example sends five ping packets to host **10.1.1.1** from **10.1.1.2:**

```
[local]Redback>ping 10.1.1.1


PING 10.1.1.1 (10.1.1.1): source 10.1.1.2, 56 data bytes,
timeout is 1 second
.!!!!
----10.1.1.1 PING Statistics----
5 packets transmitted, 4 packets received, 20.0% packet loss
round-trip min/avg/max/stddev = 0.000/0.000/0.000/0.000 ms
```

# 1.70 ping ancp

**ping ancp** {**agent-circuit-id** | **subscriber** | **circuit**} *string* [**count** *num* [**timeout** *interval*]]

## 1.70.1 Purpose

Sends an Access Node Control Protocol (ANCP) General Switch Management Protocol (GSMP) port management message to the ANCP neighbor peer to test the peer.

## 1.70.2 Command Mode

- exec (10)

## 1.70.3 Syntax Description

| | |
|---|---|
| **agent-circuit-id** *string* | Circuit agent ID. A text string, with up to 255 printable characters; enclose the string in quotation marks (“ ”) if the string includes spaces. |
| **subscriber** *string* | Subscriber name. A text string in the format *sub-name@ctx-name* with the @ the default separator character. |
| **circuit** *string* | Circuit ID. A text string in the format slot/port [circuit-id], where the *circuit-id* argument is one of the following constructs:<br>• **vlan** *pvc-vlan-id*—Virtual LAN (VLAN) tag value of a permanent virtual circuit (PVC) that is not within an 802.1Q tunnel<br>• **vlan** *tunl-vlan-id*—VLAN tag value of an 802.1Q tunnel.<br>• **vlan** *tunl-vlan-id*:*pvc-vlan-id*—VLAN tag value for the tunnel followed by the VLAN tag value for the PVC within the tunnel.<br>The range of values for any VLAN tag value is 1 to 4,095. |
| **count** *num* | Number of operations, administration, and maintenance (OAM) loopback cells the neighbor peer (the digital subscriber line [DSL] access multiplexer [DSLAM]) is to use to test the line. The range of values is 1 to 32; the default value is 5. |
| **timeout** *interval* | Maximum number of seconds the DSLAM must wait for the command to finish transmitting. The range of values is 0 to 255; the default value is 10. |

## 1.70.4 Default

None

## 1.70.5 Usage Guidelines

Use the **ping ancp** command to send an ANCP GSMP port management message to the ANCP neighbor peer to test the peer.

When entered with the **subscriber** *string* construct, the **ping ancp** command limits the search to the context in which you are working. Before entering the **ping ancp** command, ensure that you are working in the context to which the subscriber is bound.

The SmartEdge router holds the CLI prompt until either a result is received from the DSLAM or the timeout (plus one second) occurs. Any reply from the DSLAM is displayed by the CLI if it is received by the SmartEdge router before the timeout occurs; if the reply is received after the timeout, it is written to the log as an informational message.

Table 24 lists the code field values.

*Table 24 Code Field Values*

| Code Field Value | Description |
|---|---|
| 0x500 | Specified access line does not exists |
| 0x501 | Loopback test timed out |
| 0x502 | Reserved |
| 0x503 | DSL line status showtime |
| 0x504 | DSL line status idle |
| 0x505 | DSL line status silent |
| 0x506 | DSL line status training |
| 0x507 | DSL line integrity error |
| 0x508 | Access Node resource not available |
| 0x509 | Invalid test parameter |

## 1.70.6 Examples

The following example sends **10** OAM cells in an GSMP port management message to the ANCP neighbor peer, using the circuit for subscriber **joe@isp1** with a timeout interval of **15** seconds:

```
[local]Redback#ping ancp subscriber joe@isp1 count 10 timeout 15
```

# 1.71 ping arp

**ping arp** ***dest-ip-address*** **bridge** ***bridge-name*** [**context** ***context_name***] **source** ***source-ip-address*** [**retries** ***number-of-retries***] [**timeout** ***seconds***]

## 1.71.1 Purpose

Initiates an ARP request from the PE to all access circuits (ACs) and PWs that are configured between the source PE and the destination CPE.

## 1.71.2 Command Mode

exec

## 1.71.3 Syntax Description

| | |
|---|---|
| ***dest-ip-address*** | Specifies the destination IP address to use for the ping in the format ***A.B.C.D***. |
| **bridge** ***bridge-name*** | Name of the bridge that contains the MAC address. |
| **context** ***context-name*** | Optional. Name of the context that contains the bridge. |
| **source** ***source-ip-address*** | Specifies the source IP address to use for the ping in the format ***A.B.C.D***. |
| **retries** ***number-of-retries*** | Optional. Specifies the number of times ARP can be unresponsive before the ping fails. The default number of retries is *4*. |
| **timeout** ***seconds*** | Optional. Specifies the number of seconds to wait for an ARP response from the CPE before the ping fails. The default number of seconds is *1*. |

## 1.71.4 Default

None

## 1.71.5 Usage Guidelines

Use the **ping arp** command to initiate an ARP request from the PE to all access circuits (ACs) and PWs that are configured between the source PE and the destination CPE.

Consider the following restrictions before using the **ping arp** command to troubleshoot problems in a bridging domain:

- The **ping arp** command does not work over transport circuits in a bridge.
- The **ping arp** command does not work if a BVI is configured in a bridge.

## 1.71.6 Examples

The following example shows what happens when a CPE ping is aborted because the PE does not receive an ARP response from the CPE:

```
[local]Redback#ping arp 1.0.0.10 1.0.0.8 bridge br1
PING 1.0.0.10 (1.0.0.10): source 1.0.0.8
ARP Timeout!
```

# 1.72 ping atm

**`ping atm`** {**`channel`** | **`path`**} {**`end-to-end`** | **`segment`**} ***`slot/port`*** [**`vpi`**] ***`vpi`*** [[**`vci`**] ***`vci`***] [**`count`** ***`number`***] [**`timeout`** ***`seconds`***]

## 1.72.1 Purpose

Tests Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) by sending operation, administration, and maintenance (OAM) loopback cells.

## 1.72.2 Command Mode

- exec

## 1.72.3 Syntax Description

| | |
|---|---|
| **`channel`** | Sends F5 OAM loopback cells. |
| **`path`** | Sends F4 OAM loopback cells. |
| **`end-to-end`** | Sends OAM loopback cells to the end of the connection where ATM cells are terminated. |
| **`segment`** | Sends OAM loopback cells to a neighbor switch. |
| ***`slot`*** | Chassis slot number of the ATM line card with the port to be tested. |
| ***`port`*** | Port number of the ATM port to be tested. |
| ***`start-vpi`*** | Optional. Starting virtual path identifier (VPI). The range of values is 0 to 255. |
| **`through`** ***`end-vpi`*** | Optional. Last VPI in the range. |
| ***`start-vci`*** | Optional. Starting virtual circuit identifier (VCI). The range of values is 1 to 65535. By convention, values 1 to 30 are reserved for system use. |
| ***`end-vci`*** | Optional. Last VCI in the range. |
| **`count`** ***`number`*** | Optional. Number of OAM cells to send. The range of values is 1 to 10000; the default value is 5. |
| **`timeout`** ***`seconds`*** | Optional. Time in seconds that the SmartEdge router waits for a response for each OAM ping and the interval between which OAM ping packets are sent. The range of values is 1 to 100; the default value is 1. |

## 1.72.4 Default

Sends 5 OAM cells every 12 seconds over the specified VP.

## 1.72.5 Usage Guidelines

Use the **`ping atm`** command to test ATM PVCs by sending OAM loopback cells. This command tests the reachability of a neighboring ATM switch or the end of an ATM connection.

**Note:** The SmartEdge 100 router limits the value of the ***slot*** argument to 2.

**Note:** The value for the ***port*** argument on the SmartEdge 100 router depends on the MIC slot in which the ATM OC MIC is installed.

The SmartEdge router does not allow multiple administrators to ping the same ATM PVC at the same time. When one administrator is running a ping on an ATM PVC, no other administrators are able to run a ping on that same PVC until the first is finished. The following error message is issued if you are trying to ping an ATM PVC that is running the ping of another administrator: **Outstanding ping is in progress on this pvc, ping not available.**

Use the **path** keyword to send F4 OAM loopback cells; use the **channel** keyword to send F5 OAM loopback cells.

The ! character in the output of the ping command indicates a successful packet; a period (.) indicates a failed one.

**Note:** To test the reachability of a host, use the **ping** command in exec mode.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

## 1.72.6 Examples

The following example shows how to send 16 end-to-end F5 cells on VPI:VCI **2:47** on ATM port **1** in slot **5:**

```
[local]Redback>ping atm channel end-to-end 5/1 vpi 2 vci 47 count 16


Sending 16, end-to-end F5 cells on 5/1, 2:47, timeout is 2 seconds:
!!!!!!!!!!!!!!!!
Success rate is 100 percent (16/16)
```

# 1.73 ping cpe

```
ping cpe [ number-of-pings] dest-ip-address source-ip-address
bridge bridge-name [arp-retries number-of-retries] [arp-timeout
seconds] [context context_name] [icmp-timeout seconds] [maxs
max-sweep-size] [mins mins-sweep-size] [pattern hex-pattern}] [size
datagram-size] [ttl ttl-value] [verbose]
```

## 1.73.1 Purpose

Initiates a (CPE) ping to a CPE to troubleshoot problems in the VPLS network and determine the CPE host location.

## 1.73.2 Command Mode

exec

## 1.73.3 Syntax Description

| | |
|---|---|
| *number-of-pings* | Optional. Specifies the number of pings to transmit. The default number of pings transmitted is 4. |
| *dest-ip-address* | Specifies the destination IP address to use for the ping in the format ***A.B.C.D***. |
| *source-ip-address* | Specifies the source IP address to use for the ping in the format ***A.B.C.D***. |
| `bridge` *bridge-name* | Name of the bridge that contains the MAC address. |
| `arp-retries` *number-of-retries* | Optional. Specifies the number of times ARP can be unresponsive before the pir fails. The default number of retries is 4. |
| `arp-timeout` *seconds* | Optional. Specifies the number of seconds to wait for an ARP response from the before the ping fails. The default number of seconds is 1. |
| `context` *context-name* | Optional. Name of the context that contains the bridge. |
| `icmp-timeout` *seconds* | Optional. Number of seconds to wait for an ICMP response from the CPE before the ping fails. The default is 1 second. |
| `maxs` *max-sweep-size* | Optional. Minimum range of packet sizes to send, in bytes. |
| `mins` *mins-sweep-size* | Optional. Maximum range of packet sizes to send, in bytes. |
| `pattern` *hex-pattern* | Optional. Hexadecimal pattern to use for filling in the ICMP packet. |
| `size` *datagram-size* | Optional. Size of the ICMP datagram. |
| `ttl` *ttl-value* | Optional. Time-to-live (TTL) value for the IP packet. Normally, the IP packet TTL propagated to the MPLS label header at the ingress of the LSP. The TTL value a places an upper limit on the number of pseudo-wires that are traversed to trace a address. The default TTL is 64. |
| `verbose` | Optional. Displays more detailed output. |

## 1.73.4 Default

None

## 1.73.5 Usage Guidelines

Use the **ping cpe** command troubleshoot problems in the VPLS network and determine the CPE host location.

The **ping cpe** command can be used to perform the following tasks:

- Discover an IP host address
- Detect duplicate IP addresses
- Troubleshoot the data path to the host

Consider the following restrictions before using the **ping cpe** command to troubleshoot problems in a bridging domain:

- The **ping cpe** command does not work over transport circuits in a bridge.
- The **ping cpe** command does not work if a BVI is configured in a bridge.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

## 1.73.6 Examples

The following example shows how to initiate a CPE ping to discover an IP host address and troubleshoot the data path to the host. In this example, the CPE ping is successful, and there are no duplicate IP addresses configured in the system:

```
[local]Redback#ping cpe 1.0.0.10 1.0.0.8 bridge br1
PING 1.0.0.10 (1.0.0.10): source 1.0.0.8
CPE MAC 22:6a:43:00:22:01
36 data bytes,
timeout is 1 second
!!!!!
----1.0.0.10 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.900/1.224/1.762/0.440 ms
```

The following example shows what happens when a CPE ping is aborted because the PE does not receive an ARP response from the CPE:

```
[local]Redback#ping cpe 1.0.0.10 1.0.0.8 bridge br1
PING 1.0.0.10 (1.0.0.10): source 1.0.0.8
ARP Timeout!
```

# 1.74 ping ipv6

**ping** { [**ipv6**] *ipv6-addr* | **ipv6** *hostname*} [*number-of-packets*] [**flood**] [**hop-limit** *num-hops*] [**numeric**] [**pattern** *hex-pattern*] [**preload**] [**quiet**] [**record**] [**silent**] [**size** *bytes*] [**source** *ipv6-addr*] [**timeout** *seconds*] [**verbose**] [**gateways** *gateway-list*]

## 1.74.1 Purpose

Tests whether the host is reachable.

## 1.74.2 Command Mode

- exec

## 1.74.3 Syntax Description

| | |
|---|---|
| *ipv6-addr* | IP address of the host. |
| *hostname* | Name of the host. |
| *number-of-packets* | Optional. Number of ping packets to send. The range of values is 1 to 2,147,483,647; the default value is 5. |
| **flood** | Optional. Floods ping packets. |
| **hop-limit** *num-hops* | Insert a hop limit for the ping in the IPv6 header of the ping packet. The range of values is from 1 to 255. |
| **numeric** | Optional. Specifies numeric output only. |
| **pattern** *hex-pattern* | Optional. Hexadecimal pattern to fill in Internet Control Message Protocol version 6 (ICMPv6) packets. The range of values is 0x0 to 0xffff. |
| **silent** | Optional. Displays only summary lines at start up. |
| **size** *bytes* | Optional. Size, in bytes, of the IPv6 datagram, excluding the IPv6/ICMPv6 header. The range of values is 8 to 18,024; the default value is 8. |
| **source** *ipv6-addr* | Optional. Source IPv6 address. |
| **timeout** *seconds* | Optional. Interval, in seconds, that the system waits for a response for each ping packet. The range of values is 1 to 120; the default value is 1. |
| **verbose** | Optional. Enables all possible output. |
| **gateways** *gateway-list* | Optional. A list of gateway IPv6 addresses or hostnames. |

## 1.74.4 Default

Sends 8-byte packets to the specified host, using a timeout value of 1 second.

## 1.74.5 Usage Guidelines

Use the **ping ipv6** command (in exec mode) to test whether the host is reachable.

**Note:** When an IPv6 address is specified, the `ipv6` keyword is optional. The `ipv6` keyword is required if a hostname is specified.

Press **Ctrl+C** to stop a ping test.

You can only use the ***`hostname`*** argument if DNS is enabled via the **`ip domain-lookup`**, **`ip domain-name`**, and **`ip name-servers`** commands (in context configuration mode). For more information about these commands, see *Configuring DNS*.

The **`ping ipv6`** and **`traceroute ipv6`** commands (in exec mode) can display vastly different output, depending on the context in which the commands are issued. In particular, an IP address that can be reached by the **`ping ipv6`** or **`traceroute ipv6`** command in one context might not be reachable from another context. Use the **`context`** command (in exec mode) to switch between contexts.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

Table 25 lists the ICMPv6 type and ICMP codes that can be displayed in the output.

*Table 25 ICMP Error and Message Code Descriptions*

| ICMPv6 Type | ICMP Code |
|---|---|
| Destination Unreachable - 1 | No Route - 0<br>Adminstratively Prohibited - 1<br>Beyond Scope of Source Address - 2<br>Unreachable Address - 3<br>Unreachable No Port - 4 |
| Packet Too Big - 2 | 0 |
| Time Exceeded - 3 | Exceeded Transit - 0<br>Exceeded Reassembly - 1 |
| Parameter Problem - 4 | Header Problem - 0<br>Next Header Problem - 1<br>Option Unrecognized - 2 |

## 1.74.6 Examples

The following example sends five ping packets to host `2001:a:1:2::1` from `2002:a:1:2::2`:

```
[local]Redback>ping ipv6 2001:a:1:2::1 source 2002:a:1:2::2


PING 2001:a:1:2::1 (2001:a:1:2::1): source 2002:a:1:2::2, 8 data bytes,
timeout is 1 second, source 2002:a:1:2::2
.!!!!
----2001:a:1:2::1 PING6 Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/std-dev = 1.520/1.837/2.008/0.182 ms
```

# 1.75 ping mpls ldp

**ping mpls ldp** ***endpoint-ip-addr/prefix-length*** [***count***] [**exp** ***exp-bits***] [**interval** ***interval***] [**pad** ***hex-pad***] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**size** ***packet-size*** | **sweep** ***start-size end-size increment***] [**source** ***ip-addr***] [**source-port** {**any** | **mpls-ping** | ***udp-port***}] [**timeout** ***interval***] [**ttl** ***ttl-value***] [**verbose**]

## 1.75.1 Purpose

Initiates a Multiprotocol Label Switching (MPLS) ping across a Label Distribution Protocol (LDP) label-switched path (LSP).

## 1.75.2 Command Mode

exec

## 1.75.3 Syntax Description

| | |
|---|---|
| `ldp` *`endpoint-ip-addr/prefix-length`* | IP address of the egress LSR (in the form `A.B.C.D)` and prefix length, separated by the slash (`/`) character. The range of values for the *`prefix-length`* argument is 0 to 32. |
| *`count`* | Optional. Number of times that the ping is to be repeated. |
| `exp` *`exp-bits`* | Optional. IP precedence for the IP packet. Normally, the IP precedence is propagated to the MPLS label experimental (EXP) bits. |
| `interval` *`interval`* | Optional. Interval, in milliseconds, between ping requests; the default value is 0. |
| `pad` *`hex-pad`* | Optional. Hexadecimal pattern used to fill the echo request to the packet size; the default value is *0xacee*. |
| `pad-reply-mode` | Optional. Specifies whether the echo reply is returned with the hexadecimal pattern used to fill the echo request. |
| `copy` | Specifies that the echo reply should include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is copied from the echo request to the echo reply. |
| `drop` | Specifies that the echo reply should not include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is dropped. |
| `reply-mode` | Optional. Specifies how the LSP echo reply is returned. |
| `router-alert` | Sends the echo reply as an IP User Datagram Protocol (UDP) packet, with the router alert option preceding the IP header. |
| `udp` | Sends the echo reply as an IP UDP packet, with no router alert option preceding the IP header. |
| `size` *`packet-size`* | Optional. Packet size for the ping request. The ping request is filled using the Pad type-length-value (TLV) to satisfy the request; the default value is 100 bytes. |
| `sweep` | Optional. Specifies the range of packet sizes to send. The value of the *`count`* argument specifies the number of times the entire range of packet sizes is to be sent. |

| | |
|---|---|
| *start-size* | Initial sweep packet size, in bytes. |
| *end-size* | Final sweep packet size, in bytes. |
| *increment* | Packet size increase, in bytes, between packet sends. The packet size is incremented until the value of the ***end-size*** argument is either met or would be exceeded by an additional increment. |
| source *ip-addr* | Optional. Source IP address to use for the ping. If no IP address is specified, an IP interface address is selected. |
| source-port | Optional. Specifies the source UDP port for the LSP ping request. By default, port 3503 is used as the source UDP port. |
| any | Uses an unused UDP source port, selected from the reserved range of ports, as the source UDP port. |
| mpls-ping | Uses port 3503 as the source UDP port. |
| *udp-port* | Source UDP port specified within the non-reserved range of ports. The range of non-reserved ports is from 1,024 to 65,535. |
| timeout *interval* | Optional. Interval, in seconds, to wait for an LSP ping response. The default value is 1 second. |
| ttl *ttl-value* | Optional. Time-to-live (TTL) value for the IP packet. Normally, the IP packet TTL is propagated to the MPLS label header at the ingress of the LSP. |
| verbose | Optional. Displays more detailed output. |

### 1.75.4 Default

None

### 1.75.5 Usage Guidelines

Use the **ping mpls** command to initiate a MPLS ping across an LDP LSP.

Enter the command on the ingress label-switched router (LSR) for the LSP being tested, with the egress LSR as the target. (The endpoint IP address is typically the loopback address where the LSP terminates.)

**Note:** Backup LSPs cannot be pinged with MPLS.

An MPLS ping tests the connectivity of the MPLS LSP data plane, and verifies that the information in the control plane is consistent with the data plane.

MPLS Echo Request and MPLS Echo Reply messages are used to accomplish the MPLS ping. An MPLS Echo Request message, which follow the same data path that normal MPLS traffic would traverse, is sent from the LSP ingress to the LSP egress LSR. The egress LSR replies with an echo request, which, because LSPs are unidirectional, takes the routed IP path.

**Note:** The router issuing the **ping mpls** command must be the ingress LSR for the LSP being tested. The target is the egress LSR.

**Note:** For the MPLS ping-specified TTL to be set in the MPLS label, TTL propagation must not be disabled. Use the **propagate ttl ip-to-mpls** command under router mpls configuration mode to enable TTL propagation.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

### 1.75.6 Examples

The following example sends an MPLS ping across an LDP LSP with the endpoint 100.1.1.3/32 to be sent once:

```
[local]Redback#ping mpls ldp 100.1.1.3/32 1
Sending 5 100-byte MPLS echos to LDP 100.1.1.3/32, source 100.1.1.3,
    timeout is 1 second, send interval is 0 msec:
!!!!!
```

The following example sends an MPLS ping across an LDP LSP with endpoint 3.3.3.3/32. Verbose output is requested:

```
[local]Redback#ping mpls ldp 3.3.3.3/32 verbose

Sending 5 100-byte MPLS echos to LDP 3.3.3.3/32, source 3.3.3.1,
    timeout is 1 second, send interval is 0 msec:
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 5.193/6.800/11.491/2.670 ms
```

## 1.76 ping mpls mac-address

**ping mpls mac-address** ***mac-addr*** **bridge** ***bridge-name*** [**context** ***context-name***] [***count***] [**exp** ***exp-bits***] [**interval** ***interval***] [**pad** ***hex-pad***] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**size** ***packet-size*** | **sweep** ***start-size end-size increment***] [**source** ***ip-addr***] [**source-port** {**any** | **mpls-ping** | ***udp-port***}] [**timeout** ***interval***] [**trace**] [**ttl** ***ttl-value***] [**verbose**]

### 1.76.1 Purpose

Initiates a MPLS ping or a trace to a medium access control (MAC) address in a Virtual Private LAN Services (VPLS) network.

### 1.76.2 Command Mode

exec

### 1.76.3 Syntax Description

| | |
|---|---|
| ***mac-addr*** | MAC address of the host in the form ***nn:nn:nn:nn:nn:nn***. |
| **bridge** ***bridge-name*** | Name of the bridge that contains the MAC address. |
| **context** ***context-name*** | Name of the context that contains the bridge. |
| ***count*** | Optional. Number of times that the ping is to be repeated. |
| **exp** ***exp-bits*** | Optional. IP precedence for the IP packet. Normally, the IP precedence is propagated to the MPLS label experimental (EXP) bits. |
| **interval** ***interval*** | Optional. Interval, in milliseconds, between ping requests; the default value is 0. |
| **pad*****hex-pad*** | Optional. Hexadecimal pattern used to fill the echo request to the packet size; the default value is 0xacee. |
| **pad-reply-mode** | Optional. Specifies whether the echo reply is returned with the hexadecimal pattern used to fill the echo request. |
| **copy** | Specifies that the echo reply should include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is copied from the echo request to the echo reply. |
| **drop** | Specifies that the echo reply should not include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is dropped. |
| **reply-mode** | Optional. Specifies how the LSP echo reply is returned. |
| **router-alert** | Sends the echo reply as an IP User Datagram Protocol (UDP) packet, with the router alert option preceding the IP header. |
| **udp** | Sends the echo reply as an IP UDP packet, with no router alert option preceding the IP header. |
| **size** ***packet-size*** | Optional. Packet size for the ping request. The ping request is filled using the Pad type-length-value (TLV) to satisfy the request; the default value is 100 bytes. |
| **sweep** | Optional. Specifies the range of packet sizes to send. The value of the ***count*** argument specifies the number of times the entire range of packet sizes is to be sent. |

| | |
|---|---|
| *start-size* | Initial sweep packet size, in bytes. |
| *end-size* | Final sweep packet size, in bytes. |
| *increment* | Packet size increase, in bytes, between packet sends. The packet size is incremented until the value of the ***end-size*** argument is either met or would be exceeded by an additional increment. |
| source *ip-addr* | Optional. Source IP address to use for the ping. If no IP address is specified, an IP interface address is selected. |
| source-port | Optional. Specifies the source UDP port for the LSP ping request. By default, port 3503 is used as the source UDP port. |
| any | Uses an unused UDP source port, selected from the reserved range of ports, as the source UDP port. |
| mpls-ping | Uses port 3503 as the source UDP port. |
| *udp-port* | Source UDP port specified within the non-reserved range of ports. The range of non-reserved ports is from 1,024 to 65,535. |
| timeout *interval* | Optional. Interval, in seconds, to wait for an LSP ping response. The default value is 1 second. |
| trace | Optional. Requires all intermediate nodes in a multihop topology to reply to the MPLS ping request. |
| ttl *ttl-value* | Optional. Time-to-live (TTL) value for the IP packet. Normally, the IP packet TTL is propagated to the MPLS label header at the ingress of the LSP. The TTL value also places an upper limit on the number of pseudo-wires that are traversed to trace a MAC address. |
| verbose | Optional. Displays more detailed output. |

### 1.76.4 Default

None

### 1.76.5 Usage Guidelines

Use the **ping mpls mac-address** command to initiate an MPLS ping or a trace to a MAC address in a VPLS network.

Performing an MPLS MAC ping helps to verify whether a specific MAC address has been learned over an access circuit attached to a VPLS network. The VPLS provider edge (PE) router that hosts the MAC's attachment circuit replies to the MPLS MAC ping request.

The MAC address and the VPLS Bridge instance name must be specified for an MPLS MAC ping request.

When issuing this command, the MAC address and the VPLS bridge name must be specified; the context name is required if the VPLS bridge instance resides in a different context.

**Note:**

The implementation of this command supports the following proprietary features that do not support customer premise equipment (CPE) interoperability:

- Ping requests are sent over the outer MPLS tunnel instead of the inner tunnel (pseudo-wire) using proprietary TLVs. Other CPEs that do not support this scheme ignore this option.

- If the **`verbose`** keyword is specified, additional information about the pseudo-wire is requested and returned using proprietary TLVs.

**Note:** The router issuing the **`ping mpls mac-address`** command must have a bridge that is a part of the VPLS.

**Note:** For the MPLS ping-specified TTL to be set in the MPLS label, TTL propagation must not be disabled. Use the **`propagate ttl ip-to-mpls`** command under router mpls configuration mode to enable TTL propagation.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

### 1.76.6 Examples

The following example initiates an MPLS ping to MAC address, **00:00:c0:01:01:42**, on the VPLS bridge, **BridgeName1:**

```
[local]Redback#ping mpls mac-address 00:00:c0:01:01:42 bridge BridgeName1


Sending 5 100-byte MPLS echos to 2.2.2.2 for MAC 00:00:c0:01:01:42 LDP PWID 1,
source 1.1.1.1,
    timeout is 1 second, send interval is 0 msec:
!!!!!


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 4.744/5.263/6.382/0.641 ms [local]puppy#
ping mpls mac-address 00:00:c0:01:01:42 bridge BridgeName1 trace interval 15 Sending 5 100-byte MPLS
echos to 2.2.2.2 for MAC 00:00:c0:01:01:42 LDP PWID 1, source 1.1.1.1,
    timeout is 1 second, send interval is 15 msecs:
!!!!!


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 4.277/5.431/8.598/1.789 ms [local]puppy#
ping mpls mac-address 00:00:c0:01:01:42 bridge BridgeName1 trace sweep 100 500 10
Sending 5 [100-500]-byte MPLSechos to 2.2.2.2 for MAC 00:00:c0:01:01:42 LDP PWID 1,
source 1.1.1.1,
    timeout is 1 second, send interval is 0 msec:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


---- MPLS PING Statistics----
205 packets transmitted, 205 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 3.953/5.070/31.873/2.043 ms
```

The following example initiates an MPLS ping to MAC address, **00:00:c0:01:01:42**, on the VPLS bridge, **BridgeName1**, and requests a reply in a verbose (detailed) format:

```
[local]Redback#ping mpls mac-address 00:00:c0:01:01:42 bridge BridgeName1 verbose


    MAC info
Context          Bridge Group     MAC              Circuit
local            BridgeName1      00:00:c0:01:01:42 VPLS 2


VPLS peer (bridge/ip:pwid):  BridgeName1/2.2.2.2:1
 Oper State          : Up           Context name        : local
 Admin State         : Enable       Circuit id          : VPLS 2
 Peer Flags : active, pw-up
 Bridge id           : 0x2          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131072       PW encap type       : Ethernet
 PW Out label        : 131075       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Sending 5 100-byte MPLS echos to 2.2.2.2 for MAC 00:00:c0:01:01:42
LDP PWID 1, source 1.1.1.1,
    timeout is 1 second, send interval is 0 msec:
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
    MAC info
Context          Bridge Group     MAC              Circuit
0x40080001       BridgeName1      00:00:c0:01:01:42 9/3:1023:63/1/1/483
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
    MAC info
Context          Bridge Group     MAC              Circuit
0x40080001       BridgeName1      00:00:c0:01:01:42 9/3:1023:63/1/1/483
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
    MAC info
Context          Bridge Group     MAC              Circuit
0x40080001       BridgeName1      00:00:c0:01:01:42 9/3:1023:63/1/1/483
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
    MAC info
```

```
Context          Bridge Group     MAC              Circuit
0x40080001       BridgeName1      00:00:c0:01:01:42 9/3:1023:63/1/1/483
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
    MAC info
Context          Bridge Group     MAC              Circuit
0x40080001       BridgeName1      00:00:c0:01:01:42 9/3:1023:63/1/1/483


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 8.028/9.090/11.353/1.352 ms
```

# 1.77 ping mpls pw

To ping a specific virtual circuit (VC) that is associated with an Label Distribution Protocol (LDP) Layer 2 VPN (L2VPN) cross-connection:

**ping mpls pw vc-id** *vc-id* **peer** *ip-addr* [*count*] [**exp** *exp-bits*] [**interval** *interval*] [**pad** *hex-pad*] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**send-mode** {**control-plane** | **data-plane**] [**size** *packet-size* | **sweep** *start-size end-size increment*] [**source** *ip-addr*] [**source-port** {**any** | **mpls-ping** | *udp-port*}] [**timeout** *interval*] [**ttl** *ttl-value*] [**verbose**]

To ping a pseudowire (PW) using the inner label that is associated with a static L2VPN cross-connection:

**ping mpls pw vpn-label** *label-num* **peer** *ip-addr* [*count*] [**exp** *exp-bits*] [**interval** *interval*] [**pad** *hex-pad*] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**size** *packet-size* | **sweep** *start-size end-size increment*] [**source** *ip-addr*] [**source-port** {**any** | **mpls-ping** | *udp-port*}] [**timeout** *interval*] [**ttl** *ttl-value*] [**verbose**]

To ping a specific PW:

**ping mpls pw pw-id** *pw-num* **peer** *ip-addr* [*count*] [**exp** *exp-bits*] [**interval** *interval*] [**pad** *hex-pad*] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**send-mode** {**control-plane** | **data-plane**}] [**size** *packet-size* | **sweep** *start-size end-size increment*] [**source** *ip-addr*] [**source-port** {**any** | **mpls-ping** | *udp-port*}] [**timeout** *interval*] [**ttl** *ttl-value*] [**verbose**]

## 1.77.1 Purpose

Tests the status of a PW.

## 1.77.2 Command Mode

exec

## 1.77.3 Syntax Description

| | |
|---|---|
| `vc-id` *`vc-id`* | Virtual circuit (VC) ID associated with the LDP L2VPN cross-connection. The range of the *`vc-id`* argument value is 0 to 4,294,967,295. |
| `vpn-label` *`label-num`* | Inner label associated with the static L2VPN cross-connection. The range of the *`label-num`* argument values is 4,096 to 65,535. |
| `pw-id` *`pw-num`* | Pseudo-wire ID. The value of the *`pw-num`* argument is a 4-byte number. The range of the *`pw-num`* argument value is 0 to 4,294,967,295. |
| `peer` *`ip-addr`* | Remote provider edge (PE) router's IP address in the form *`A.B.C.D`*. |
| *`count`* | Optional. Number of times that the ping is to be repeated. |

| | |
|---|---|
| **exp** ***exp-bits*** | Optional. IP precedence for the IP packet. Normally, the IP precedence is propagated to the MPLS label experimental (EXP) bits. |
| **interval** ***interval*** | Optional. Interval, in milliseconds, between ping requests; the default value is 0. |
| **pad** ***hex-pad*** | Optional. Hexadecimal pattern used to fill the echo request to the packet size; the default value is *0xacee*. |
| **pad-reply-mode** | Optional. Specifies whether the echo reply is returned with the hexadecimal pattern used to fill the echo request. |
| **copy** | Specifies that the echo reply should include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is copied from the echo request to the echo reply. |
| **drop** | Specifies that the echo reply should not include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is dropped. |
| **reply-mode** | Optional. Specifies how the LSP echo reply is returned. |
| **router-alert** | Sends the echo reply as an IP User Datagram Protocol (UDP) packet, with the router alert option preceding the IP header. |
| **udp** | Sends the echo reply as an IP UDP packet, with no router alert option preceding the IP header. |
| **send-mode** | Optional. Specifies whether the ping is sent over the control plane or data plane. By default, the ping is sent over the data plane. |
| **control-plane** | Sends the ping over the control plane. |
| **data-plane** | Sends the ping over the data plane. This setting is the default. |
| **size** ***packet-size*** | Optional. Packet size for the ping request. The ping request is filled using the Pad type-length-value (TLV) to satisfy the request; the default value is 100 bytes. |
| **sweep** | Optional. Specifies the range of packet sizes to send. The value of the ***count*** argument specifies the number of times the entire range of packet sizes is to be sent. |
| ***start-size*** | Initial sweep packet size, in bytes. |
| ***end-size*** | Final sweep packet size, in bytes. |
| ***increment*** | Packet size increase, in bytes, between packet sends. The packet size is incremented until the value of the ***end-size*** argument is either met or would be exceeded by an additional increment. |
| **source** ***ip-addr*** | Optional. Source IP address to use for the ping. If no IP address is specified, an IP interface address is selected. |
| **source-port** | Optional. Specifies the source UDP port for the LSP ping request. By default, port 3503 is used as the source UDP port. |
| **any** | Uses an unused UDP source port, selected from the reserved range of ports, as the source UDP port. |
| **mpls-ping** | Uses port 3503 as the source UDP port. |
| ***udp-port*** | Source UDP port specified within the non-reserved range of ports. The range of non-reserved ports is from 1,024 to 65,535. |
| **timeout** ***interval*** | Optional. Interval, in seconds, to wait for an LSP ping response. The default value is 1 second. |
| **ttl** ***ttl-value*** | Optional. Time-to-live (TTL) value for the IP packet. Normally, the IP packet TTL is propagated to the MPLS label header at the ingress of the LSP. |
| **verbose** | Optional. Displays more detailed output. |

### 1.77.4 Default

None

### 1.77.5 Usage Guidelines

Use the **`ping mpls pw`** command to test the status of a pseudo-wire.

The remote PE router replies to a MPLS pseudo-wire ping message with its local information about the pseudo-wire. You can use this information for troubleshooting purposes to compare the state and attributes at the two ends of a pseudo-wire.

The IP address of the remote PE router and the VC ID, inner label, or pseudo-wire ID must be specified for an MPLS pseudo-wire ping request. An MPLS pseudo-wire ping is initiated only if a pseudo-wire with the specified attributes exists.

**Note:**

The implementation of this command supports the following proprietary features that do not support customer premise equipment (CPE) interoperability:

- Ping requests are sent over the outer MPLS tunnel instead of the inner tunnel (pseudo-wire) using proprietary TLVs. Other CPEs that do not support this scheme ignore this option.
- If the **`verbose`** keyword is specified, additional information about the pseudo-wire is requested and returned using proprietary TLVs.

**Note:** The router issuing the **`ping mpls pw`** command must be the ingress LSR for the LSP being tested.

**Note:** For the MPLS ping-specified TTL to be set in the MPLS label, TTL propagation must not be disabled. Use the **`propagate ttl ip-to-mpls`** command under router mpls configuration mode to enable TTL propagation.

**Note:** If you do not use the **`send-mode`** keyword to manually configure the ping send mode, the SmartEdge router sends the ping over the data plane by default. In SmartEdge router releases before Release 6.1.3, the SmartEdge router sent the ping over the control plane by default.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

### 1.77.6 Examples

The following example shows how to test the pseudo-wire with the 1 pseudo-wire ID and request that the remote PE router with the **2.2.2.2** IP address reply with its local information about the pseudowire:

```
[local]Redback#ping mpls pw pw-id 1 peer 2.2.2.2


Sending 5 100-byte MPLS echos to 2.2.2.2 for LDP PWID 1, source 1.1.1.1,
timeout is 1 second, send interval is 0 msec:
!!!!!


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 3.791/4.206/5.043/0.485 ms
```

The following example shows how to test the pseudo-wire with the **1** pseudo-wire ID and request that the remote PE router with the **2.2.2.2** IP address reply with its local information about the pseudowire in a verbose (detailed) format:

```
[local]Redback#ping mpls pw pw-id 1 peer 2.2.2.2 verbose


VPLS peer (bridge/ip:pwid):  BridgeName1/2.2.2.2:1
 Oper State          : Up           Context name        : local
 Admin State         : Enable       Circuit id          : VPLS 2
 Peer Flags : active, pw-up
 Bridge id           : 0x2          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131072       PW encap type       : Ethernet
 PW Out label        : 131075       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Sending 5 100-byte MPLS echos to 2.2.2.2 for LDP PWID 1, source 1.1.1.1,
    timeout is 1 second, send interval is 0 msec:
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up
Received MPLS ping reply - None


VPLS peer (bridge/ip:pwid):  BridgeName1/1.1.1.1:1
 Oper State          : Up           Context name        : 0x40080001
 Admin State         : Enable       Circuit id          :
255/21:1023:63/0/1/8
 Peer Flags : active, pw-up
 Bridge id           : 0x3          Context id          : 0x40080001
 PE peering type     : Hub          PE local mode       : PE-rs
 Prev state          : Down         Profile name        : test1
 Prev event          : pw-up        Last error          : no error
 Peer up/down cnt    : 1            Peer state changes  : 2
 Peer reset cnt      : 0            Peer config changes : 0
 Peer restart cnt    : 0            Peer proc restarts  : 0
 MAC flush sent      : 0            MAC flush received  : 0
 Circ up/down cnt    : 0            Circ cfg changes    : 1
 Circ error cnt      : 0            Circ delete cnt     : 0
 PW state            : Up, Active
 PW up/down cnt      : 0            PW signaling type   : LDP
 PW error cnt        : 0            PW restart cnt      : 1
 PW In label         : 131075       PW encap type       : Ethernet
 PW Out label        : 131072       PW Exp bits         : 0x0
 PW local MTU        : 1500         PW remote MTU       : 1500
 PW flags  : in-rib, in-lblmap, in-ldp, from-ldp, from-cfg
             peer-up


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 7.311/8.758/9.851/1.185 ms
```

# 1.78 ping mpls rsvp

**ping mpls rsvp** *lsp-name* [*count*] [**exp** *exp-bits*] [**interval** *interval*] [**pad** *hex-pad*] [**pad-reply-mode** {**copy** | **drop**}] [**reply-mode** {**router-alert** | **udp**}] [**size** *packet-size* | **sweep** *start-size end-size increment*] [**source** *ip-addr*] [**source-port** {**any** | **mpls-ping** | *udp-port*}] [**timeout** *interval*] [**ttl** *ttl-value*] [**verbose**]

## 1.78.1 Purpose

Initiates a MPLS ping across a Resource Reservation Protocol (RSVP) label-switched path (LSP) or a Label Distribution Protocol (LDP) LSP.

## 1.78.2 Command Mode

exec

## 1.78.3 Syntax Description

| | |
|---|---|
| *lsp-name* | Name of the RSVP LSP to be pinged; an LSP that originates on your router and ends on another node (the number of transit hops is not important). The local router must be the LSP ingress router. |
| *count* | Optional. Number of times that the ping is to be repeated. |
| **exp** *exp-bits* | Optional. IP precedence for the IP packet. Normally, the IP precedence is propagated to the MPLS label experimental (EXP) bits. |
| **interval** *interval* | Optional. Interval, in milliseconds, between ping requests; the default value is 0. |
| **pad** *hex-pad* | Optional. Hexadecimal pattern used to fill the echo request to the packet size; the default value is *0xacee*. |
| **pad-reply-mode** | Optional. Specifies whether the echo reply is returned with the hexadecimal pattern used to fill the echo request. |
| **copy** | Specifies that the echo reply should include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is copied from the echo request to the echo reply. |
| **drop** | Specifies that the echo reply should not include the hexadecimal pattern used to fill the echo request. The hexadecimal pattern is dropped. |
| **reply-mode** | Optional. Specifies how the LSP echo reply is returned. |
| **router-alert** | Sends the echo reply as an IP User Datagram Protocol (UDP) packet, with the router alert option preceding the IP header. |
| **udp** | Sends the echo reply as an IP UDP packet, with no router alert option preceding the IP header. |
| **size** *packet-size* | Optional. Packet size for the ping request. The ping request is filled using the Pad type-length-value (TLV) to satisfy the request; the default value is 100 bytes. |
| **sweep** | Optional. Specifies the range of packet sizes to send. The value of the *count* argument specifies the number of times the entire range of packet sizes is to be sent. |
| *start-size* | Initial sweep packet size, in bytes. |

| | |
|---|---|
| *end-size* | Final sweep packet size, in bytes. |
| *increment* | Packet size increase, in bytes, between packet sends. The packet size is incremented until the value of the ***end-size*** argument is either met or would be exceeded by an additional increment. |
| `source` *ip-addr* | Optional. Source IP address to use for the ping. If no IP address is specified, an IP interface address is selected. |
| `source-port` | Optional. Specifies the source UDP port for the LSP ping request. By default, port 3503 is used as the source UDP port. |
| `any` | Uses an unused UDP source port, selected from the reserved range of ports, as the source UDP port. |
| `mpls-ping` | Uses port 3503 as the source UDP port. |
| *udp-port* | Source UDP port specified within the non-reserved range of ports. The range of non-reserved ports is from 1,024 to 65,535. |
| `timeout` *interval* | Optional. Interval, in seconds, to wait for an LSP ping response. The default value is 1 second. |
| `ttl` *ttl-value* | Optional. Time-to-live (TTL) value for the IP packet. Normally, the IP packet TTL is propagated to the MPLS label header at the ingress of the LSP. |
| `verbose` | Optional. Displays more detailed output. |

### 1.78.4 Default

None

### 1.78.5 Usage Guidelines

Use the **`ping mpls rsvp`** command to initiate an MPLS ping across an RSVP LSP.

Enter the command on the ingress label-switched router (LSR) for the LSP being tested. The name of the target LSP should be an LSP that originates on your node and ends on another node (the number of transit hops is not important). You cannot ping an egress or a transit RSVP LSP.

You can use the **`show rsvp lsp`** command to look up names of RSVP LSPs to ping.

**Note:** Backup LSPs cannot be MPLS pinged.

An MPLS ping tests the connectivity of the MPLS LSP data plane, and verifies that the information in the control plane is consistent with the data plane.

MPLS Echo Request and MPLS Echo Reply messages are used to accomplish the MPLS ping. An MPLS Echo Request message, which follows the same data path that normal MPLS traffic would traverse, is sent through the LSP that leads to the LSP egress LSR. The egress LSR replies with an echo request, which, because LSPs are unidirectional, takes the routed IP path.

**Note:** The router issuing the **`ping mpls rsvp`** command must be the ingress LSR for the LSP being tested.

**Note:** For the MPLS ping-specified TTL to be set in the MPLS label, TTL propagation must not be disabled. Use the **propagate ttl ip-to-mpls** command under router mpls configuration mode to enable TTL propagation.

**Note:** When pinging at a high rate, some pings are dropped due to rate limiting. This is normal behavior.

### 1.78.6 Examples

The following example sends an MPLS ping across RSVP LSP, **lsp1:**

```
[local]Redback#ping mpls rsvp lsp1


Sending 5 100-byte MPLS echos to lsp1, source 3.3.3.3,
    timeout is 1 second, send interval is 0 msec:
!!!!!


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 2.223/3.125/3.853/0.676 ms
```

The following example sends an MPLS ping across RSVP LSP, **pse_pe2**. Verbose output is requested:

```
[local]Redback#ping mpls rsvp pse_pe2 verbose


Sending 5 100-byte MPLS echos to pse_pe2, source 3.3.3.3,
    timeout is 1 second, send interval is 0 msec:
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1
Received MPLS ping reply - Replying router is an egress for FEC at level 1


---- MPLS PING Statistics----
5 packets transmitted, 5 packets received no error, 0.0% packet loss/error
round-trip min/avg/max/stddev = 5.193/6.800/11.491/2.670 ms
```

## 1.79 policy access-list

To create a policy access list to be applied to packets associated with a forward policy, a NAT policy, or QoS metering or policing policy:

**policy access-list** *acl-name* [**permit** | **seq** *seq-num* **permit**} [*protocol*] {*src src-netmask* | **any** | **host** *src*} {*dest dest-netmask* | **any** | **host** *dest*} {**class** *class-name* **cond** *cond-id* | **dscp eq** *dscp-value* | **fragments class** *class-name* **cond** *cond-id* | **ip-options class** *class-name* **cond** *cond-id* | **length** *packet-length* [*operator* | **range** *begin-packet-length end-packet-length*] | **precedence** *prec-value* | **tos** *tos-value*]]

To remove a policy access-list:

```
[no] policy access-list acl-name
```

To create or remove a policy access list to be applied to SSH and telnet session packets:

```
[no] policy access-list ssh-and-telnet-acl
```

To add or remove a description for an existing policy access-list:

```
[no] policy access-list acl-name description line
```

### 1.79.1 Command Mode

context configuration

### 1.79.2 Syntax Description

| | |
|---|---|
| `acl-name` | Name of the policy access-list |
| `permit` | Specifies that the criteria defined in the command are permitted when the ACL is processed.<br>Create subsequent rules using the `permit` command in access control list configuration mode. |
| `seq` *`seq-num`* `permit` | Numbers the first permit rule with a sequence number. Create subsequent rules using the `seq` command in access control list configuration mode. |
| *`protocol`* | Optional. Number indicating a protocol as specified in RFC 1700, *Assigned Numbers*. The range of values is 0 to 255 or one of the keywords listed in Table 8. |
| *`src`* | Source address to be included in the permit criteria. An IP address in the form *`A.B.C.D`*. |
| *`src-netmask`* | Indication of which bits in the *`source`* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the *`src-netmask`* argument must be matched by the corresponding bits in the *`src`* argument. For any one-bits in the *`src-netmask`* argument, the corresponding bits in the *`src`* argument are ignored. |
| `any` | Specifies any source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255. |
| `host` *`source`* | IP address of a specific single-host. |

| | |
|---|---|
| *cond* | Optional. Matching condition for the **class** argument. One of the following:<br>• Condition ID—with values from 1 to 4294967295<br>• Condition ID in IP address format, A.B.C.D |
| *port* | Optional. Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source or destination port. This argument is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 10 and Table 11. |
| **range** *port end-port* | Optional if you specify the TCP or UDP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must be within the specified range to match the criteria. The range of values is 1 to 65,535 or one of the keywords listed in Table 10 and Table 11. |
| **max-sessions** *limit* | Optional. Maximum number of sessions allowed for the specified IP address or IP subnet. This construct is only available for TCP. Use the **ip access-list** command with the **ssh-and-telnet-acl** keyword to apply an IP ACL to packets associated with an Secured Shell (SSH) or a Telnet server. The range of values is 1 to 32. |
| **min-sessions** *limit* | Optional. Minimum number of sessions allowed for the specified IP address or IP subnet. This construct is only available if you specify TCP as the protocol in this command and use the **ip access-list** command with the **ssh-and-telnet-acl** keyword to apply an IP ACL to packets associated with an SSH or a Telnet server. The range of values is 0 to 32.<br>The sum of values specified for the **min-sessions** *limit* construct for all specified IP addresses or IP subnets must not exceed 32. |
| *dest* | Optional. Destination address to be included in the permit or deny criteria. An IP address in the form *A.B.C.D*. |
| *dest-netmask* | Indication of which bits in the *dest* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the *dest-wildcard* argument must be matched by the corresponding bits in the *dest* argument. For one-bits in the *dest-wildcard* argument the corresponding bits in the *dest* argument are ignored. |
| **length** *length* | Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header, regardless of the specified protocol. The range of values for the packet length is 20 to 65,535. For the operators, see the |

| | |
|---|---|
| *operator* | Optional. Operator for the **length** keyword. One of the following:<br>• eq—Equal to<br>• gt—Greater than<br>• lt—Less than<br>• neq—Not equal to |
| **range** *length* **end-length** | Packets that fall into the range of specified lengths. Each value (*length* and ***end-length***) can be from 20 to 65,535. |
| **host** *dest* | A a single-host destination with no network mask. The *dest* argument is an IP address in the A.B.C.D format. |
| **icmp-type** *icmp-type* | This argument is only available if you specify the ICMP protocol. Type of Internet Control Message Protocol (ICMP) packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 12. |
| **icmp-code** *icmp-code* | Optional if you use the **icmp-type** *icmp-type* construct. A particular ICMP message code to be matched. The range of values is 0 to 255. |
| **igmp-type** *igmp-type* | This argument is only accepted if you specified **igmp** as the *protocol* argument. Type of Internet Group Management Protocol (IGMP) packet to be matched. The range of values is 0 to 15 or one of the keywords listed in Table 13. |
| **dscp eq** *dscp-value* | Optional. Packet's Differentiated Services Code Point (DSCP) value must be equal to the value specified in the *dscp-value* argument to match the criteria. The range of values is 0 to 63 or one of the keywords listed in Table 14. |
| **established** | Optional. Specifies that only established connections are to be matched. This keyword is only available if you specified **tcp** for the *protocol* argument. |

| | |
|---|---|
| **invalid-tcp-flags** | Optional. Specifies that TCP packets with flag combinations other than the following are a match:<br>• SYN<br>• SYN+ACK<br>• ACK<br>• PSH+ACK<br>• URG+ACK<br>• URG+PSH+ACK<br>• FIN<br>• FIN+ACK<br>• RST<br>• RST+ACK<br>Only the lower-order 6 bits (for example, FIN, SYN, RST, PSH, ACK, and URG) in the TCP Flags field are considered for validation. The higher order 6-bits (ECN bits defined by RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, and the reserved bits) are ignored.<br>This keyword is only available if you specify **tcp** for the ***protocol*** argument. |
| **setup** | Optional. Specifies that TCP packets with SYN set and ACK not set in the Flags field are a match.<br>This keyword is only available if you specify **tcp** for the ***protocol*** argument. |
| **precedence** ***prec-value*** | Optional. Precedence value of packets to be considered a match. The range of values is 0 to 7, 7 (the highest precedence) or one of the keywords listed in Table 15. |
| **tos** ***tos-value*** | Optional. Type of service (ToS) to be considered a match. The range of values is 0 to 15 or one of the keywords listed in Table 16. |
| **fragments** | Optional. Allows packet to be permitted or denied based on whether the packet is fragmented. This keyword matches packets where the More-Fragments field is equal to 1 or the IP-Offset field is not equal to 0.<br>You can also add a class with condition rules with this keyword. |

| | |
|---|---|
| `ip-options` | Optional. Specifies that IPv4 packets with the IP Header Length field is greater than 20 are a match. You can also add a class with condition rules with this keyword. |
| `class` *`class-name`* | Optional. Policy-based class name. |
| *`cond`* | Optional. Matching condition for the `class` argument. One of the following:<br>• Condition ID—with values from 1 to 4294967295<br>• Condition ID in IP address format, A.B.C.D |
| `condition` *`cond-id`* | Optional. Matching condition for the `class` argument. One of the following:<br>• Condition ID—with values from 1 to 4,294,967,295<br>• Condition ID in IP address format, A.B.C.D |

### 1.79.3 Default

None

### 1.79.4 Purpose and Usage Guidelines

Creates or selects a policy access control list (ACL) and enters access control list configuration mode.

If a forward policy, Network Address Translation (NAT) policy, or quality of service (QoS) policy references a policy ACL that does not exist, the reference is ignored.

You can enter the **`policy access-list`** command in one string with the **`permit`** or **`seq`** *`seq-num`* **`permit`** keywords, or create the policy access-list (with the **`policy access-list`** *`acl-name`* construct). Whether you include the first rule in the command or not, you can then use the **`permit`** or **`seq`** commands in access control list configuration mode to configure the remainder of the rules.

To create a policy ACL to process SSH and Telnet packets, enter the command with the **`ssh-and-telnet-acl`** keyword (enters access control list configuration mode). Then use the **`permit`** or **`seq`** *`seq-num`* **`permit`** commands to configure the rules.

**Note:** This command applies only to IPV4 ACLs.

Use the **`no`** form of this command to remove the policy ACL.

*Table 26 Valid Keyword Values for the length operator Argument*

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

### 1.79.5 Examples

The following example creates a policy ACL to define **Web** and **VOIP** traffic types on a circuit, and uses the policy ACL in a QoS metering policy, marking these packet types as **DF** and **AF11**, respectively. All other traffic is marked as **DF**:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list QoSACL-1
[local]Redback(config-access-list)#permit tcp any any eq 80 class Web
[local]Redback(config-access-list)#permit udp any any eq 1000 class VOIP
[local]Redback(config-access-list)#permit any any class default
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#qos policy PolicingAndMarking metering
[local]Redback(config-policy-metering)#ip access-group QoSACL-1 local
[local]Redback(config-policy-group)#class Web
[local]Redback(config-policy-group-class)#mark dscp DF
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class VOIP
[local]Redback(config-policy-group-class)#mark dscp AF11
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class default
[local]Redback(config-policy-group-class)#mark dscp DF
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-metering)#exit
[local]Redback(config)#port ethernet 3/0
[local]Redback(config-port)#bind interface FromSubscriber local
[local]Redback(config-port)#qos policy policing PolicingAndMarking
```

## 1.80 policy-refresh

**policy-refresh** {**username** *subscriber* | **agent-remote-id** *id* **attribute** *name* {*value* **[parent] [remove]**}

### 1.80.1 Purpose

Modifies in real time a subscriber attribute in the specified subscriber record, using the command-line interface (CLI).

### 1.80.2 Command Mode

- exec (10)

### 1.80.3 Syntax Description

| | |
|---|---|
| `username` *`subscriber`* | Fully qualified subscriber name, in the format *`sub-name@ctx-name`*, for which the attribute is to be modified. |
| `agent-remote-id` *`id`* | Remote Authentication Dial-In User Service (RADIUS) remote agent ID, for which the attribute is to be modified. An alphanumeric string of up to 63 characters. |
| `attribute` *`name`* | Subscriber attribute to be updated. Table 27 lists the keyword names for the attributes and the related RADIUS standard attribute or vendor-specific attribute (VSA) provided by Ericsson AB. |
| *`value`* | New value for the subscriber attribute, according to the arguments, constructs, and parameter types listed in Table 27. If the value is to be *`remove`*, enclose it in double quotation marks (“ ”). |
| `remove` | Removes the subscriber attribute from the subscriber record. |
| `parent` | Optional. Applies the modification of a `dynamic-qos-param` attribute to the parent circuit of the subscriber session instead of the subscriber session. The `remove` keyword can also be specified with the `parent` keyword to remove the parent `dynamic-qos-param` attribute. |

### 1.80.4 Default

Subscriber attributes are unchanged for the duration of the session, unless modified by the **`reauthorize`** command (in exec mode).

### 1.80.5 Usage Guidelines

Use the **`policy-refresh`** command to modify in real time a subscriber policy attribute in the specified subscriber record, using the CLI. Policy refresh does not interrupt or drop the session of the subscriber.

To modify a **`dynamic-qos-param`** attribute of the parent circuit of the subscriber session, use the **`parent`** keyword with the **`policy-refresh`** configuration. The **`parent`** keyword enables dynamic QoS parameter support for parent circuits through subscriber sessions. Using this keyword, you can customize QoS configurations of a parent circuit of a subscriber session by using the **`policy-refresh`** command. When the subscriber session is specified in a **`policy-refresh`** command that includes the **`parent`** keyword, any specified modification is applied to the parent circuit instead of the subscriber session. The parent circuit of a subscriber session is considered to be the 802.1q VLAN or ATM PVC which encapsulates its traffic and under which the **`bind authentication`** or **`bind subscriber`** CLI configuration entry of the subscriber was specified. Modifications to the QoS configurations of the parent circuit may apply to all traffic (all subscriber sessions) that traverse the circuit depending on the configuration of the QoS policy binding of the parent. (for example, whether that binding is inherited by its children; see *Policy Inheritance* in *Configuring QoS Rate-Limiting and Class- Limiting*).

**Note:** All the children (subscriber sessions) should agree on the value of any dynamic QoS parameter that they specify to be applied to their common parent. When the value of a dynamic QoS parameter conflicts among the children, then the last value to be received from RADIUS or otherwise specified (for example, through the **`policy-refresh`** command) is the one that is enforced.

For predictable system behavior, the following rules apply:

- All the children (subscriber sessions) must agree on the absolute value of any dynamic QoS parameter that they specify be applied to their common parent.

- Disagreement about the value of any dynamic QoS parameter among the children has the following effects:

- The last parent dynamic QoS parameter received for any applicable subscriber session overrides the previously applied QoS parameter value.

- When a subscriber session goes down or applicable attribute is removed, depending on the various conflicting values and their order of application, one of the following may happen: The parent dynamic QoS parameter value continues to remain in effect, or the currently applied dynamic QoS parameter value is removed, and the enforced attribute value reverts back to the statically configured value.

- If any of the following processes are restarted while disagreement exists for the value of a parent-flagged attribute among the children of a common parent, any of the conflicting values may be applied after the process is recovered: AAA, RCM, QoS.

- If QoS rate parameters conflict, the precedence is as follows:

  The last dynamic QoS parameter (VSA 196) rate applied to the parent circuit or an applicable child using the parent flag takes precedence over the last applied VSA 156 or 157 rate applied to the parent circuit.

  The final rate to be enforced is the lower of the last ANCP or TR-101 rate update received or the AAA (RADIUS or policy-refresh) rate specified, as determined by the preceding rule.

- If neither an ANCP or TR-101 nor an AAA (RADIUS or policy refresh) rate has been applied, then the static configuration rate is enforced; for example, the rate specified in the policy or the **`rate circuit`** command, if applicable.

**Note:** This command and the **`reauthorize`** command (in exec mode) each perform the same function. However, the **`reauthorize`** command uses the RADIUS authentication process to perform the update instead of the CLI.

For more information about RADIUS and vendor VSAs provided by Ericsson AB, refer to *Configuring RADIUS*.

Table 27 lists the keywords and constructs, parameter types for the attribute keyword **`dynamic-qos-param`** and their range of values, for the subscriber attributes that this command supports.

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| **`bridge-profile`** | | String. Name of the bridge profile. | 102 |
| **`dhcp-max-leases`** | | Integer. Maximum number of DHCP addresses this subscriber can allocate to hosts; the range of values is 1 to 1,255. | 3 |
| **`dynamic-qos-param`** | **`fwd-in-access-group`** | String. Name of one or more IPv4 policy ACLs to be referenced by the subscriber's RADIUS-guided inbound forward policy. The format is:<br>*`<acl-name1>:<acl-name2>:<acl-name3>:...:<acl-name10>`*<br>where *`acl-name`* is the name of the policy ACL created using the **`policy access-list`** command (in context configuration mode). This command supports a maximum of 10 ACLs. For example, the acl1:acl2:acl3 string references ACLs named ACL1, ACL2, and ACL3.(1) | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **`ipv6-fwd-in-access-group`** | String. Name of one or more IPv6 policy ACLs to be referenced by the subscriber's RADIUS-guided inbound forward policy. The format is:<br>*`<acl-name1>:<acl-name2>:<acl-name3>:...:<acl-name10>`*<br>where ***`acl-name`*** is the name of the policy ACL created using the **`ipv6 policy access-list`** command (in context configuration mode). This command supports a maximum of 10 ACLs. For example, the acl1:acl2:acl3 string references ACLs named ACL1, ACL2, and ACL3.[2] | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **`meter-circuit-burst`** | String. Overrides the circuit burst parameter defined by a metering policy and set with the **`rate`** command. This attribute is used to configure the metering burst allowance for the specified circuit. The format is:<br>**`meter-circuit-burst`** ***`bytes`***<br>where the ***`bytes`*** argument is the burst tolerance in bytes. The range of values is 1 to 4250000000. The **`meter-circuit-burst`** parameter is not accepted unless a rate and burst are configured in the metering policy of the target circuit.<br>This attribute is used to configure the metering burst allowance for the subscriber circuit. The range of allowable values is from 1 to 4,250,000,000 bytes.<br>meter-circuit-excess-burst <value | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
|  | **meter-circuit-conform** | String. Overrides the circuit conform parameters defined by a metering policy. This attribute is used to configure marking action for packets that conform to the circuit-level rate and burst allowance of a metering policy. The format is:<br>**meter-circuit-conform** {{**mark-dscp** ***dscp-value***} \| {**mark-precedence** ***prec-value***} \| {**mark-priority** ***priority-value***} \| **no-action**}<br>where:<br>- **mark-dscp** ***dscp-value*** corresponds to the **conform mark dscp** command (in policy rate configuration mode). The ***dscp-value*** argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **conform mark dscp** command.<br>- **mark-precedence** ***prec-value*** corresponds to the **conform mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>- **mark-priority** ***priority-value*** corresponds to the **conform mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>- **no-action** corresponds to the **conform no-action** command (in policy rate configuration mode). The **meter-circ** | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **meter-circuit-exceed** | String. Overrides the circuit exceed parameters defined by a metering policy. This attribute is used to configure marking action for packets that exceed the circuit-level rate and burst allowance of a metering policy. The format is:<br>**meter-circuit-exceed** {{**mark-dscp** ***dscp-value***} \| {**mark-precedence** ***prec-value***} \| {**mark-priority** ***priority-value***} \| {**drop-qos-priority** ***priority-value***} \| **drop-all** \| **no-action**}<br>where:<br>• **mark-dscp** ***dscp-value*** corresponds to the **exceed mark dscp** command (in policy rate configuration mode). The ***dscp-value*** argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **exceed mark dscp** command.<br>• **mark-precedence** ***prec-value*** corresponds to the **exceed mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** ***priority-value*** corresponds to the **exceed mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>• **drop-qos-priority** ***priority-value*** corresponds to the **exceed drop qos-priority** | 196 |

Table 27 Subscriber Attributes Supported by Policy Refresh

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-circuit-excess-burst` | String. Overrides the circuit excess burst parameter defined by a metering policy and set with the **`rate`** command (in metering policy configuration mode). This attribute is used to configure the metering excess-burst allowance for the specified circuit. The format is:<br>**`meter-circuit-excess-burst`** ***`bytes`***<br>where the ***`bytes`*** argument is the excess burst tolerance in bytes. The range of values is 1 to 4250000000. The **`meter-circuit-excess-burst`** parameter is not accepted unless a rate and excess-burst are configured in the metering policy of the target circuit.<br>This attribute is used to configure the metering excess-burst allowance for the subscriber circuit. The range of allowable values is from 1 to 4,250,000,000 bytes. meter-circuit-excess-burst <value> | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-circuit-mark` | String. Overrides the circuit mark parameter defined by a metering policy. This attribute is used to configure an unconditional marking action for packets subject to a metering policy. The format is:<br>**meter-circuit-mark** {**mark-dscp** ***dscp-value*** \| **mark-precedence** ***prec-value*** \| **mark-priority** ***priority-value***}<br>where:<br>• **mark-dscp** ***dscp-value*** corresponds to the **mark dscp** command (in policy rate configuration mode). The ***dscp-value*** argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **mark dscp** command.<br>• **mark-precedence** ***prec-value*** corresponds to the **mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** ***priority-value*** corresponds to the **mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>This attribute is used to configure an unconditional marking action for packets subject to the metering policy. meter-circuit-mark {mark-dscp \| mark-precedence \| mark-priority} <0-7><br>The **meter-circuit-mark** parameter is not accepted if a rate is | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-circuit-rate` | String. Overrides the circuit rate parameter defined by a metering policy and set with the **rate** command. This attribute is used to configure the metering rate of the subscriber circuit. The format is:<br>**meter-circuit-rate rate-absolute** ***rate-value***<br>where the ***rate-value*** argument is the ***kbps*** argument of the **rate** command (in metering policy configuration mode). The range of values is 5 to 10000000. The **meter-circuit-rate** parameter is not accepted unless a rate and burst are configured in the metering policy of the target circuit.<br>This attribute is used to configure metering rate of the subscriber circuit. The range of allowable values is from 5 to 10,000,000 kbps. meter-circuit-rate <value> | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **meter-circuit-violate** | String. Overrides the circuit violate parameters defined by a metering policy. This attribute is used to configure marking action for packets that violate the circuit-level rate and excess-burst allowance of a metering policy. The format is:<br>**meter-circuit-violate** {**mark-dscp** *dscp-value* \| **mark-precedence** *prec-value* \| **mark-priority** *priority-value*} \| **drop-all** \| **no-action**}<br>where:<br>• **mark-dscp** *dscp-value* corresponds to the **violate mark dscp** command (in policy rate configuration mode). The *dscp-value* argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **violate mark dscp** command.<br>• **mark-precedence** *prec-value* corresponds to the **violate mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** *priority-value* corresponds to the **violate mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>• **drop-all** corresponds to the **violate drop** command (in policy rate configuration mode).<br>• **no-action** corresponds | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-class-burst` | String. Overrides the class burst parameter defined by a metering policy. The format is:<br>***class-name*** **burst** ***bytes***<br>where ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition and the **burst** ***bytes*** construct is the burst tolerance in bytes. The range of values for the **burst** argument is 1 to 1250000000. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-class-conform` | String. Overrides the class conform values defined by a metering policy. The format is:<br>*`class-name mark-dscp mark-precedence mark-priority no-action`*<br>where:<br>• *`class-name`* is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• *`mark-dscp`* is the *`dscp-class`* argument of the **`conform mark dscp`** command (in policy rate configuration mode). The *`dscp-class`* argument is an integer from 0 to 63 or a DSCP keyword.<br>• *`mark-precedence`* is the *`prec-value`* argument of the **`conform mark precedence`** command (in policy class rate configuration mode). The range of values is 1 to 3.<br>• *`mark-priority`* is the *`group-num`* argument of the **`qos priority`** and **`conform mark priority`** command (in policy class rate configuration mode). The range of values is 0 to 7.<br>• *`no-action`* corresponds to the **`conform no-action`** command (in policy class rate configuration mode). | 196 |

Table 27 Subscriber Attributes Supported by Policy Refresh

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **meter-class-exceed** | String. Overrides the class exceed parameters defined by a metering policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority drop-qos-priority drop-all no-action***<br>where:<br>- ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>- ***mark dscp*** is the ***dscp-class*** argument of the **exceed mark dscp** command (in policy class rate configuration mode). The ***dscp-class*** argument is an integer from 0 to 63 or a DSCP keyword.<br>- ***mark-precedence*** is the ***prec-value*** argument of the **exceed mark precedence** command (in policy class rate configuration mode). The range of values is 1 to 3.<br>- ***mark-priority*** is the ***group-num*** argument of the **exceed mark priority** command (in policy class rate configuration mode). The range of values is 0 to 7.<br>- ***drop-qos-priority-group*** is the ***group-num*** argument of the **qos priority** command. The range of values is 0 to 7. Supported modes are: ATM OC configuration, ATM PVC configuration, dot1q PVC configuration, Frame Relay PVC configuration, link group configuration, | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-class-excess-burst` | String. Overrides the class excess burst parameter defined by a metering policy set with the **`rate`** command (in metering policy configuration mode). The format is:<br>***`class-name`*** **`excess-burst`** ***`bytes`***<br>where the ***`class-name`*** argument is the name of the class assigned to policy ACL statements that reference the ACL condition, and the **`excess-burst`** ***`bytes`*** construct is the excess burst tolerance in bytes. The range of values for the ***`bytes`*** argument is 1 to 1250000000. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **meter-class-mark** | String. Overrides the class mark parameter defined by a metering policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority***<br>where:<br>• ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***mark-dscp*** is the ***dscp-class*** argument of the **mark dscp** command (in metering policy configuration mode).<br>• ***mark-precedence*** is the ***prec-value*** argument of the **mark precedence** command (in metering policy configuration mode). The range of values is 1 to 3.<br>• ***mark-priority*** is the ***group-num*** argument of the **mark priority** command (in metering policy configuration mode).<br>(3) | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `meter-class-rate` | String. Overrides the class rate parameter defined by a metering policy. The format is:<br>***`class-name rate-value`***<br>where the ***`class-name`*** argument is the name of the class assigned to policy ACL statements that reference the ACL condition, and the ***`rate-value`*** argument is the ***`kbps`*** argument of the **`rate`** command (in metering policy configuration mode). | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **`meter-class-violate`** | String. Overrides the class violate parameters defined by a metering policy. The format is:<br>***`class-name mark-dscp mark-precedence mark-priority`*** [**`drop-all`**] [**`no-action`**]<br>where:<br>• ***`class-name`*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***`mark-dscp`*** is the ***`dscp-class`*** argument of the **`violate mark dscp`** command (in policy class rate configuration mode).<br>• ***`mark-precedence`*** is the ***`prec-value`*** argument of the **`violate mark precedence`** command (in policy class rate configuration mode).<br>• ***`mark-priority`*** is the ***`group-num`*** argument of the **`violate mark priority`** command (in policy class rate configuration mode).<br>• **`drop-all`**–Drop all packets that match the configured violate parameters.<br>• **`no-action`**—No marking is taken on packets that conform to the configured violate parameters. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-circuit-burst` | String. Overrides the circuit burst parameter defined by a policing policy. This attribute is used to configure the policing burst allowance for the subscriber circuit. The format is:<br>**`police-circuit-burst`** ***`bytes`***<br>where the ***`bytes`*** argument is the burst tolerance in bytes. The range of values is 1 to 4250000,000.<br>This attribute is used to configure the policing burst allowance for the subscriber circuit. The range of allowable values is from 1 to 4,250,000,000 bytes. police-circuit-burst <value> | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **`police-circuit-conform`** | String. Overrides the circuit conform parameters defined by a policing policy. This attribute is used to configure marking action for packets that conform to the circuit-level rate and burst allowance of the metering policy. The format is:<br>**police-circuit-conform** {**mark-dscp** *dscp-value* \| **mark-precedence** *prec-value* \| **mark-priority** *priority-value*} \| **no-action**}<br>where:<br>• **mark-dscp** *dscp-value* corresponds to the **conform mark dscp** command (in policy rate configuration mode). The *dscp-value* argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **conform mark dscp** command.<br>• **mark-precedence** *prec-value* corresponds to the **conform mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** *priority-value* corresponds to the **conform mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>• **no-action** corresponds to the **conform no-action** command (in policy rate configuration mode). | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **police-circuit-exceed** | String. Overrides the circuit exceed parameters defined by a policing policy. This attribute is used to configure marking action for packets that exceed the circuit-level rate and burst allowance of the policing policy. The format is:<br>**police-circuit-exceed** {**mark-dscp** ***dscp-value*** \| **mark-precedence** ***prec-value*** \| **mark-priority** ***priority-value***} \| {**drop-qos-priority** ***priority-value***} \| **drop-all** \| **no-action**}<br>where:<br>• **mark-dscp** ***dscp-value*** corresponds to the **exceed mark dscp** command (in policy rate configuration mode). The **dscp-value** argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **exceed mark dscp** command.<br>• **mark-precedence** ***prec-value*** corresponds to the **exceed mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** ***priority-value*** corresponds to the **exceed mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>• **drop-qos-priority** ***priority-value*** corresponds to the **exceed drop qos-priority** | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-circuit-excess-burst` | String. Overrides the circuit excess burst parameter defined by a policing policy set with the **`rate`** command (in policing policy configuration mode). This attribute is used to configure the policing excess-burst allowance for the subscriber circuit. The format is:<br>**`police-circuit-excess-burst`** ***`bytes`***<br>where the ***`bytes`*** argument is the excess burst tolerance in bytes. The range of values is 1 to 4250000000.<br>This attribute is used to configure the policing excess-burst allowance for the subscriber circuit. The range of allowable values is from 1 to 4,250,000,000 bytes. police-circuit-excess-burst <value> | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
|  | **police-circuit-mark** | String. Overrides the circuit mark parameters defined by a policing policy. This attribute is used to configure an unconditional marking action for packets subject to the policing policy. The format is:<br>**police-circuit-mark** {**mark-dscp** ***dscp-value*** \| **mark-precedence** ***prec-value*** \| **mark-priority** ***priority-value***}<br>where:<br>• **mark-dscp** ***dscp-value*** corresponds to the **mark dscp** command (in policy rate configuration mode). The ***dscp-value*** argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **mark dscp** command.<br>• **mark-precedence** ***prec-value*** corresponds to the **mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** ***priority-value*** corresponds to the **mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>This attribute is used to configure an unconditional marking action for packets subject to the policing policy. police-circuit-mark {mark-dscp \| mark-precedence \| mark-priority} <0-7><br>This attribute is used to configure an unconditional marking action for packets | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-circuit-rate` | String. Overrides the circuit rate parameter defined by a policing policy. This attribute is used to configure policing rate of the subscriber circuit. The format is:<br>**`police-circuit-rate rate-absolute`** ***`rate-value`***<br>where the ***`rate-value`*** argument is the ***`kbps`*** argument of the **`rate`** command (in policing policy configuration mode). The range of values is 5 to 10000000.<br>This attribute is used to configure policing rate of the subscriber circuit. The range of allowable values is from 5 to 10,000,000 kbps. police-circuit-rate <value> | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-circuit-violate` | String. Overrides the circuit violate parameters defined by a policing policy. This attribute is used to configure marking action for packets that violate the circuit-level rate and excess-burst allowance of the policing policy. The format is:<br>**police-circuit-violate** {**mark-dscp** *dscp-value* \| **mark-precedence** *prec-value* \| **mark-priority** *priority-value*} \| **drop-all** \| **no-action**}<br>where:<br>• **mark-dscp** *dscp-value* corresponds to the **violate mark dscp** command (in policy rate configuration mode). The *dscp-value* argument can be an integer from 0 to 63 or a DSCP keyword. For a list of the DSCP keywords, see the **violate mark dscp** command.<br>• **mark-precedence** *prec-value* corresponds to the **violate mark precedence** command (in policy rate configuration mode). The range of values is 1 to 3.<br>• **mark-priority** *priority-value* corresponds to the **violate mark priority** command (in policy rate configuration mode). The range of values is 0 to 7.<br>• **drop-all** corresponds to the **violate drop** command (in policy rate configuration mode).<br>• **no-action** corresponds | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-burst` | String. Overrides the class burst parameter defined by a policing policy. The format is:<br>**`burst`** ***`bytes`***<br>where ***`class-name`*** is the name of the class assigned to policy ACL statements that reference the ACL condition and the **`burst`** ***`bytes`*** construct is the burst tolerance in bytes. The range of values is 1 to 1250000000. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-conform` | String. Overrides the class conform values defined by a policing policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority no-action***<br>where:<br>• ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***mark-dscp*** is the ***mark-dscp dscp-class*** construct of the **conform mark dscp** command (in policy rate configuration mode). The ***dscp-class*** argument can be an integer from 0 to 63 or a DSCP keyword.<br>• ***mark-precedence*** is the **mark-precedence** ***prec-value*** construct of the **conform mark precedence** command (in policy class rate configuration mode). The range of values is 1 to 3.<br>• ***mark-priority*** is the **mark-priority** ***group-num*** construct of the **qos priority** and **conform mark priority** command (in policy class rate configuration mode). The range of values is 0 to 7.<br>• ***no-action*** corresponds to the **conform no-action** command (in policy class rate configuration mode). | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-exceed` | String. Overrides the class exceed parameters defined by a policing policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority drop-qos-priority drop-all no-action***<br>where:<br>• ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***mark dscp*** is the **mark dscp** ***dscp-class*** construct of the **exceed mark dscp** command (in policy class rate configuration mode). The ***dscp-class*** argument can be an integer from 0 to 63 or a DSCP keyword.<br>• ***mark-precedence*** is the **mark precedence** ***prec-value*** construct of the **exceed mark precedence** command (in policy class rate configuration mode). The range of values is 1 to 3.<br>• ***mark-priority*** is the **mark priority** ***group-num*** construct of the **exceed mark priority** command (in policy class rate configuration mode). The range of values is 0 to 7.<br>• ***drop-qos-priority-group*** is the **qos priority** ***group-num*** command (in global configuration mode). The range of values is 0 to 7.<br>• ***drop-all*** is the **qos-priority** ***group-num*** construct | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **police-class-excess-burst** | String. Overrides the class excess burst parameter defined by a policing policy set with the rate command (in policing policy configuration mode). The format is:<br>***class-name*** **excess-burst** ***bytes***<br>where the ***class-name*** argument is the name of the class assigned to policy ACL statements that reference the ACL condition and the ***bytes*** argument is the excess burst tolerance in bytes. The range of values is 1 to 1250000000. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-mark` | String. Overrides the class mark parameter defined by a policing policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority***<br>where:<br>• ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***mark-dscp*** is the **mark dscp** ***dscp-class*** construct of the **mark dscp** command (in policing policy configuration mode). The ***dscp-class*** argument can be an integer from 0 to 63 or a DSCP keyword.<br>• ***mark-precedence*** is the **mark precedence** ***prec-value*** construct of the **mark precedence** command (in policing policy configuration mode).<br>• ***mark-priority*** is the **mark priority** ***group-num*** construct of the **mark priority** command (in policing policy configuration mode). The range of values is 0 to 7.<br>(4) | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-rate` | String. Overrides the class rate parameter defined by a policing policy. The format is:<br>***`class-name rate-value`***<br>where ***`class-name`*** is the name of the class assigned to policy ACL statements that reference the ACL condition and the ***`rate-value`*** argument is either the **`rate`** ***`kbps`*** or **`rate percentage`** ***`value`*** construct of the **`rate`** command (in metering policy configuration mode). | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | `police-class-violate` | String. Overrides the class violate parameters defined by a policing policy. The format is:<br>***class-name mark-dscp mark-precedence mark-priority drop-all no-action***<br>where:<br>• ***class-name*** is the name of the class assigned to policy ACL statements that reference the ACL condition.<br>• ***mark-dscp*** is the **mark dscp** ***dscp-class*** construct of the **violate mark dscp** command (in policy class rate configuration mode). The ***dscp-class*** argument can be an integer from 0 to 63 or a DSCP keyword.<br>• ***mark-precedence*** is the **mark precedence** ***prec-value*** construct of the **violate mark precedence** command (in policy class rate configuration mode).<br>• ***mark-priority*** is the **mark priority** ***group-num*** construct of the **violate mark priority** command (in policy class rate configuration mode). The range of values is 0 to 7.<br>• ***drop-all*** corresponds to the **violate drop** command (in policy class rate configuration mode).<br>• ***no-action*** corresponds to the **violate no-action** command (in policy class rate configuration mode). | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **pwfq-circuit-rate-min** | String. Overrides the circuit rate minimum parameter defined by a PWFQ policy set with the **rate minimum** command (in PWFQ policy configuration mode). This attribute is used to modify the target minimum rate under congestion for a circuit with a PWFQ policy binding. The format is:<br>**pwfq-circuit-rate-minimum** ***rate-value***<br>where the ***rate-value*** argument is the ***kbps*** argument of the **rate minimum** command (in PWFQ policy configuration mode). The range of values is 64 to 1000000.<br>This attribute can be used to modify the target minimum rate under congestion for a TM L2 node; that is, a circuit with a PWFQ policy binding. It corresponds to and overrides the “rate minimum” command value configured in the PWFQ policy. The range of allowable values is from 64 kbps to 1,000,000 kbps. pwfq-circuit-rate-minimum <value>.<br>The **pwfq-circuit-rate-minimum** and **pwfq-circuit-weight** dynamic QoS parameters are mutually exclusive. A circuit cannot have these two parameters configured simultaneously. | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **`pwfq-circuit-rate-max`** | String. Overrides the circuit rate maximum parameter defined by a PWFQ policy set with the **`rate maximum`** command (in PWFQ policy configuration mode). This attribute is used to modify the maximum allowed rate for a circuit with a PWFQ policy binding. The format is:<br>**`pwfq-circuit-rate-maximum`** ***`rate-value`***<br>where the ***`rate-value`*** argument is the ***`kbps`*** argument of the **`rate maximum`** command (in PWFQ policy configuration mode). The range of values is 64 to 1000000.<br>This attribute can be used to modify the maximum allowed rate for a TM L2 node; that is, a circuit with a PWFQ policy binding. It corresponds to and overrides the “rate maximum” command value configured in the PWFQ policy. The range of allowable values is from 64 kbps to 1,000,000 kbps. pwfq-circuit-rate-maximum <value>. | 196 |

*Table 27    Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
|  | **pwfq-circuit-weight** | String. Overrides the circuit weight parameter defined by a PWFQ policy set with the **weight** command (in PWFQ policy configuration mode). This attribute is used to modify the relative weight of a circuit with a PWFQ policy binding. The format is:<br>**pwfq-circuit-weight** ***weight***<br>where the ***weight*** argument corresponds to the ***weight*** argument of the **weight** command (in PWFQ policy configuration mode). The range of values is 1 to 4096.<br>This attribute can be used to modify to relative weight of a TM L2 node; that is, a circuit with a PWFQ policy binding. It corresponds to and overrides the “weight” command value configured in the PWFQ policy. The range of allowable values is from 1 to 4096. pwfq-circuit-weight <value><br>This attribute can be used to modify the target minimum rate under congestion for a TM L2 node; that is, a circuit with a PWFQ policy binding. It corresponds to and overrides the “rate minimum” command value configured in the PWFQ policy. The range of allowable values is from 64 kbps to 1,000,000 kbps. pwfq-circuit-rate-minimum <value>.<br>The **pwfq-circuit-rate-minimum** and **pwfq-circuit-weight** dynamic QoS parameters are mutually exclusive. A circuit cannot have these two parameters configured |  |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| | **pwfq-priority-group-rate** | String. Overrides the priority group rate defined by a PWFQ policy. The format is:<br>***group-num rate-value***<br>where ***group-num*** is the ***group-num*** argument of the **queue priority-group** command, and ***rate-value*** is either the **rate** ***kbps*** or **percentage** ***value*** construct from the command. | 196 |
| | **pwfq-queue-priority** | String. Overrides the queue priority defined by a PWFQ policy. The format is:<br>***queue-num priority-group weight-value***<br>where ***queue-num*** is the **queue** ***queue-num*** construct of the **queue -priority** command, ***priority-group*** is the **priority** ***group-num*** construct, and ***weight-value*** is the **weight** ***weight*** construct. | 196 |
| | **pwfq-queue-weight** | String. Overrides the queue weight defined by a PWFQ policy. The format is:<br>***queue-num weight-value***<br>where ***queue-num*** is the **queue** ***queue-num*** construct and ***weight-value*** is the **weight** ***traffic-weight*** construct the **queue weight** command | 196 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| `filter-id` | | String. Name of the ACL that filters inbound or outbound traffic in the format:<br>• `in` ***name***<br>• `out` ***name*** | 11 |
| `forward-policy` | | String. Name of the ACL that filters inbound or outbound traffic in the format:<br>• `in` ***name***<br>• `out` ***name*** | 92 |
| `http-redirect-profile-name` | | String. Name of the HTTP redirect profile (up to 32 characters). | 107 |
| `idle-timeout` | | Integer. Idle timeout in seconds; the range of values is 1 to 65,534. | 28 |
| `igmp-svc-prof-id` | | String. Name of the IGMP service profile. | 90 |
| `mcast-receive` | | Integer. Defines whether the subscriber can receive multicast packets; the range of values is:<br>• 1=NO RECEIVE<br>• 2=RECEIVE | 34 |
| `mcast-send` | | Integer. Defines whether the subscriber can send multicast packets; the range of values is:<br>• 1=NO SEND<br>• 2=SEND<br>• 3=UNSOLICITED SEND | 33 |
| `qos-metering` | | String. Name of the QoS metering policy. | 88 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| `qos-overhead` | | String. Name of the overhead profile. | 195 |
| `qos-policing` | | String. Name of the QoS policing policy. | 87 |
| `qos-queuing` | | String. Name of the QoS scheduling policy. | 89 |
| `qos-rate` | | String. Limits (in KB) for inbound or outbound traffic in the format:<br>• **in** ***limit***<br>• **out** ***limit***<br>The range of values for ***limit*** is 0 to 65,534. Zero (0) indicates an unlimited rate. | 156, 157 |
| `qos-reference` | | String. Node name, node-name index, group name, and group-name index in the format:<br>***node-name node-name index*****:*****group-name group-name index*** | 114 |
| `session-timeout` | | Integer. Session timeout in seconds; the range of values is 1 to 65,534. | 27 |

*Table 27 Subscriber Attributes Supported by Policy Refresh*

| Attribute Keyword | Parameter Types | Notes | Related VSA # |
|---|---|---|---|
| `shaping-profile-name` | | String. Name of the ATM shaping profile. | 101 |
| `traffic-limit` | | String. Limits (in KB) for inbound or outbound traffic in the format:<br>• `in` *`limit`*<br>• `out` *`limit`*<br>Limits are independent. | 113 |

*(1) The **fwd-in-access-group** parameter does not support the **parent** keyword.*

*(2) The **ipv6-fwd-in-access-group** parameter does not support the **parent** keyword.*

*(3) The **meter-class-mark** parameter is not accepted if the corresponding class in the metering policy has been configured with a rate.*

*(4) The **police-class-mark** parameter is not accepted if the corresponding class in the policing policy has been configured with a rate.*

**Note:** VSA 196 offers a superset of the functionality of VSA 156 (Qos-Rate-Inbound) and 157 (Qos-Rate-Outbound). Use either VSA 196 or the VSA 156 and 157 sets (either VSA 156 or 157 or both) to modify the circuit-level rate and associated parameters (burst and excess-burst) on a single circuit. When both VSAs are applied to the same property of a single circuit, VSA 196 takes precedence. Any property (rate, burst, or excess-burst) specified through VSA 156 or 157 is ignored while the corresponding VSA 196 attribute is in place. If the VSA 196 attribute is removed (for example, by the COA attribute removal) and either VSA 156 or 157 is still applied to the subscriber session, the previously overridden VSA or VSAs take effect.

When the same QoS rate of a circuit is subject to modification from both the DSL line rate (received through ANCP or through TR-101 PPPoE or DHCP tags) and a rate applied through VSA 156, 157, or 196 (set through RADIUS or the `policy-refresh` exec command), the lower of the last line rate received or the relevant VSA rate (as determined by the preceding precedence rule) is applied.

### 1.80.6 Examples

The following example updates the subscriber record for subscriber **joe@gold-service** to specify a different quality of service (QoS) policing policy, **police-policy:**

```
[local]Redback#policy-refresh username joe@gold-service attribute
qos-policing police-policy
```

The following example shows how to set the rate to 10000 kbps for priority-group 0 for the subscriber's PWFQ policy binding:

```
[local]Redback#policy-refresh username joe@gold-service attribute
Dynamic-Qos-Param pwfq-priority-group-rate 0 rate-absolute 10000
```

The following example shows how to set the weight to 50 for queue 3 for the subscriber's PWFQ policy binding:

```
[local]Redback#policy-refresh username joe@gold-service attribute
Dynamic-Qos-Param pwfq-queue-weight 3 50
```

The following example shows how to set the burst allowance to 1024 bytes for class name voip for the subscriber's metering policy binding:

```
[local]Redback#policy-refresh username joe@gold-service attribute
Dynamic-Qos-Param meter-class-burst voip 1024
```

The following example shows how to set the policing rate to 7000 kbps for the policing policy binding of the parent circuit of the subscriber:

```
[local]Redback#policy-refresh username joe@gold-service attribute
Dynamic-Qos-Param police-circuit-rate rate-absolute 7000 parent
```

# 1.81 pool

`pool` ***`nat-pool-name ctx-name`***

## 1.81.1 Purpose

Configures the Network Address Translation (NAT) policy or its class to use the specified pool of IP addresses for source IP address translation.

## 1.81.2 Command Mode

- NAT policy configuration
- policy group class configuration

## 1.81.3 Syntax Description

| | |
|---|---|
| *nat-pool-name* | NAT pool name. |
| *ctx-name* | Name of the context in which the NAT pool is configured. |

## 1.81.4 Default

If no action is configured for the NAT policy, by default, packets are dropped.

## 1.81.5 Usage Guidelines

Use the `pool` command to configure the NAT policy or class of packets to use the specified pool of IP addresses for packet translation.

## 1.81.6 Examples

The following example configures the NAT policy, **NAT-POLICY**, to use the pool, **NAT-POOL-DEFAULT**, configured in the **ISP** context, and configures packets classified as **NAT-CLASS-BASIC** to use the pool, **NAT-POOL-BASIC**, configured in the **ISP** context:

```
[local]Redback(config-ctx)#nat policy NAT-POLICY
[local]Redback(config-policy-nat)#pool NAT-POOL-DEFAULT ISP
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-group)#class NAT-CLASS-BASIC
[local]Redback(config-policy-group-class)#pool NAT-POOL-BASIC ISP
```

# 1.82 port atm

```
port atm slot/port

no port atm slot/port
```

## 1.82.1 Purpose

Selects an Asynchronous Transfer Mode (ATM) port and enters ATM OC configuration mode.

## 1.82.2 Command Mode

global configuration

## 1.82.3 Syntax Description

| | |
|---|---|
| *slot* | Chassis slot number of the line card. The range of values depends on the chassis in which the line card is installed; see the Line and Services Card Types and Slots section in the *Usage Guidelines* of the *card* command. |
| *port* | Line card port number. The range of values depends on the type of line card; see Table 28 of this command. |

## 1.82.4 Default

None

## 1.82.5 Usage Guidelines

Use the **port atm** command to select an ATM port of any type and enter ATM OC configuration mode.

**Note:** The SmartEdge 100 router limits the value of the *slot* argument to 2.

Table 28 lists the range of values for the *port* argument; in the table, the IR abbreviation is used for Intermediate Reach.

*Table 28 Port Ranges for ATM Line Cards*

| Line Card Type | Physical Ports | Low-Density Version | Low-Density Ports |
|---|---|---|---|
| ATM OC-3c/STM-1c | 8 | No | – |
| ATM OC-12c/STM-4c | 1 | No | – |
| ATM OC-12c/STM-4c | 2 | No | – |

**Note:** The value for the *`port`* argument on the SmartEdge 100 router ATM OC MIC is 1 or 2.

Before the port is configured, the SmartEdge OS performs a power check to determine if the chassis has sufficient unallocated power to meet the power requirements for the port's line card. If the power requirements for the line card are greater than the unallocated power resources of the chassis, the SmartEdge OS displays the following message:

```
Insufficient power available for card <card-name> in slot <slot>.
Power Required: <n> A @48V Power Available: <m> A @48V
```

In the message, *`n`* is the amperes required by the line card and *`m`* is the amperes available for assignment. In this case, the command is not included in the system configuration. However, it might be possible to configure a line card that requires less power in this slot. Use the **`show chassis power`** command with the **`inventory`** keyword to display the power requirements for each line card.

To enable the port, use the **`no shutdown`** command in ATM OC configuration mode.

Use the **`no`** form of this command to delete the port configuration from the configuration database.

### 1.82.6 Examples

The following example shows how to select port **2** on an ATM OC line card in slot **6** and enable the port:

```
[local]Redback(config)#port atm 6/2
[local]Redback(config-atm-oc)#no shutdown
```

The following example shows how to select port **1** on the ATM OC line card in slot **3** and enable the port:

```
[local]Redback(config)#port atm 3/1
[local]Redback(config-atm-ds3)#no shutdown
```

# 1.83 port bvi

```
port bvi name

no port bvi name
```

## 1.83.1 Purpose

Creates a bridged virtual interface (BVI) port to represent a pseudo circuit that supports bridging and routing in the same SmartEdge router context.

## 1.83.2 Command Mode

- configuration

## 1.83.3 Syntax Description

| | |
|---|---|
| *name* | BVI port name. |

## 1.83.4 Default

None

## 1.83.5 Usage Guidelines

Use the **port bvi** command to name a BVI port that represents the pseudo circuit. This command must be used with the **bind interface** command in the BVI context and the **bridge** command in the BVI context to create the BVI port. The BVI port supports local or nonroutable Link Layer 2 traffic that is bridged to the bridged interfaces in the same bridge group, while routable Network Layer 3 traffic is routed to other routed interfaces.

**Warning!**

Can result in system failure. Do not configure an L2 tunnel on an interface bound to a BVI port. BVI ports are compatible only with L3 forwarding and L3 tunnels.

Access, Ethernet and dot1q link groups are supported in the bridge group. Only one BVI port can be attached to a bridge group. BVI ports are supported on link groups and link groups support up to eight Ethernet ports. BVI port pseudo circuits in a bridge group are only supported on PPA2-based Ethernet cards.

PWFQ policies and aggregate shaping are not supported on BVI ports. NAT policies are not supported on bridged virtual interfaces.

This feature does not support transport ranges and VPLS circuits. Bridge groups with VPLS configured are not supported. Binding to multibind interfaces is not supported by this feature.

The **show circuit** and the **show bindings** commands display `bvi-port` when a BVI port is configured.

To monitor the port, use the **show circuit counters** command. To enable the port, use the **no shutdown** command (in port configuration mode). Use the **no** form of this command to delete the port configuration from the configuration database.

Bidirectional Forwarding Detection (BFD) on L3 BVI ports is not supported.

RSTP is not supported on BVI ports.

BVI ports support:

- OSPF
- IPv4 dynamic routing protocols (DVSR, IS-IS, BGP, RIP)
- Economical access link groups
- Noneconomical access link groups

Related Commands in other manuals are listed in the following table.

*Table 29 Related Commands in Other Manuals*

| | |
|---|---|
| `forward policy in` | `qos policy metering` |
| `forward policy out` | `qos policy policing` |

### 1.83.6 Examples

The following example shows how to create a pseudo circuit with the **port bvi** command:

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

[local]Redback(config-ctx)#bridge bvi-bridge
[local]Redback(config-bridge)#description Bridge for BVI to support
routed and bridged traffic

[local]Redback(config-ctx)#interface i1
[local]Redback(config-if)#ip address 192.168.110.1 255.255.255.0

[local]Redback(config-ctx)#interface br1 bridge
[local]Redback(config-if)#bridge name bvi-bridge

[local]Redback(config)#port bvi port-bvi
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface i1 bvi-context
[local]Redback(config-port)#bridge name bvi-bridge bvi-context

[local]Redback(config)#port eth 1/1
[local]Redback(config-port)#bind interface br1 bvi-context

[local]Redback(config)#port eth 2/1
[local]Redback(config-port)#bind interface br1 bvi-context
```

## 1.84 port channelized-oc12

See the port <port-type> command.

## 1.85 port channelized-oc3

See the port <port-type> command.

## 1.86 port channelized-stm1

See the port <port-type> command.

## 1.87 port channelized-stm4

See the port <port-type> command.

## 1.88 port ds0s

- To configure a NxDS0 subchannel multiplexed in channelized DS1 or E1 channel in a channelized OC-3, OC-12, STM-1, or STM-4 port, the syntax is:

  **port ds0s** *slot/port*:{*ds1-channel-id* | *e1-channel-id*}:*nxds0-channel-id*

- To remove the NxDS0 subchannel configurations in a channelized DS1 channel in a channelized OC-3 or OC-12 port, or the NxDS0 subchannel configurations in a channelized E1 channel in a channelized STM-1 or STM-4 port:

  **no port port ds0s** *slot/port*:{*ds1-channel-id* | *e1-channel-id*}

- To configure a NxDS0 subsubchannel multiplexed in channelized DS1 or E1 subchannel within a channelized DS3 channel, the syntax is:

  **port ds0s** *slot/port*:*ds3-channel-id*:{*ds1-channel-id* | *e1-channel-id*}:*nxds0-channel-id*

- To remove the NxDS0 subsubchannel configurations in a channelized DS1 or E1 subchannel in a channelized DS3 channel in a channelized OC-3, OC-12, STM-1 or STM-4 port:

  **no port port ds0s** *slot/port*:*ds3-channel-id*:{*ds1-channel-id* | *e1-channel-id*}

## 1.88.1 Purpose

Enters the configuration mode for a DS0 channel in either a DS3 channel, an E1 channel, or a DS1 channel.

## 1.88.2 Command Mode

- Global Configuration

  Since the NxDS0 is configured in a channelized DS3, E1, or DS1, you can also enter this command from the following modes:

- DS-3 configuration
- E1 configuration
- DS-1 configuration

## 1.88.3 Syntax Description

| | |
|---|---|
| `ds0s` | Specifies that the channel type is NxDS0, and enters the configuration mode for the DS0. |
| ***`slot`*** | The chassis slot number where the line card is installed. |
| ***`port`*** | The number of the port containing the NxDS0 subchannel. |
| ***`ds3-channel-id`*** | When the NxDS0 is multiplexed in a channelized E1 or DS1 subchannel within a channelized DS3 channel, the ***`ds3-channel-id`*** specifies that DS3 subchannel. |
| ***`e1-channel-id`*** | The ID of the channelized E1 channel (or subchannel) containing the NxDS0 channel you are configuring.<br>If the channel given by ***`e1-channel-id`*** exists, but is not a channelized E1, the configuration attempt is rejected and the following message is displayed: `incompatible subchannel type for nxds0 subchannel`. |
| ***`ds1-channel-id`*** | The ID of the channelized DS1 channel (or subchannel) containing the NxDS0 channel you are configuring.<br>If the channel given by ***`ds1-channel-id`*** exists, but is not a channelized DS1, the configuration attempt is rejected and the following message is displayed: `incompatible subchannel type for nxds0 subchannel`. |
| ***`nxds0-channel-id`*** | The ID of the NxDS0 subchannel (or subsubchannel) you are configuring. The range of values depends on whether the NxDS0 subchannel (or subsubchannel) is nested within a channelized DS1 or E1 channel:<br>• **`1-31`** for a NxDS0 channel within an channelized E1 channel (or subchannel)<br>• **`1-24`** for a NxDS0 channel within an channelized DS1 channel (or subchannel)<br>If the value of ***`nxds0-channel-id`*** is out of range, then the command is rejected and a message similar to the following is displayed: `Invalid ds0s 14/7:1:40, channel 40 is not in range 1 to 31.` |

### 1.88.4 Usage Guidelines

- If the port identified by ***port*** is configured for Packet over SONET (POS) service, POS related features (such as encapsulation type) can be configured on the channel.
- The *aug-mapping* and *channel-mapping* commands determine into which channelized ports, you can configure the NxDS0. See *Configuring Channelized Ports* for further information.

### 1.88.5 Default

No channels on the port and no service bindings to those channels.

### 1.88.6 Examples

In the following example, the `port ds0s 2/1:3:3:1` command enters port configuration mode for the first NxDS0 subsubchannel multiplexed into the third E1 subchannel which in turn is multiplexed into the third DS3 channel in a channelized STM-1 frame.

```
port channelized-stm1 2/1 pos
 no shutdown
 aug-mapping au3-no-tug
 clock-source card-reference
 !
 port channelized-ds3 2/1:3
  no shutdown
  clock-source card-reference
 !
  port e1 2/1:3:1
   no shutdown
   clock-source card-reference
   encapsulation ppp
   bind interface pos_chstm1->chds3->e1_1 redkite1
  !
  port e1 2/1:3:2
   no shutdown
   clock-source card-reference
   bind interface pos_chstm1->chds3->e1_2 redkite1
  !
  port channelized-e1 2/1:3:3
   no shutdown
   clock-source card-reference
  !
   port ds0s 2/1:3:3:1
    no shutdown
    timeslot 1-15
    encapsulation ppp
    bind interface pos_chstm1->chds3->che1->ds0s_1 redkite1
   !
   port ds0s 2/1:3:3:16
    no shutdown
    timeslot 16-31
    bind interface pos_chstm1->chds3->che1->ds0s_2 redkite1
   !
  !
 !
!
!
```

# 1.89 port {ds1 | channelized-ds1}

- To configure a DS1 channel in a channelized OC-3 or OC-12 port:

  ```
  port {ds1 | channelized-ds1} slot/port:ds1-channel-id
  ```

- To remove the DS1 channel configurations in a channelized OC-3 or OC-12 port:

  ```
  no port {ds1 | channelized-ds1} slot/port
  ```

- To configure a DS1 subchannel in a channelized DS3 channel:

  ```
  port {ds1 | channelized-ds1} slot/port:ds3-channel-id:d
  s1-channel-id
  ```

- To remove the DS1 subchannel configurations in a channelized DS3 channel:

  ```
  no port {ds1 | channelized-ds1} slot/port:ds3-channel-id
  ```

## 1.89.1 Purpose

Enters the configuration mode for a DS1 channel in a channelized OC-3 or OC-12 port or in a channelized DS3 channel.

## 1.89.2 Command Mode

- Global Configuration

  Since the DS1 is configured in a channelized OC-3, OC-12, or DS3, you can also enter this command from the following modes:

- port configuration (OC-3)
- port configuration (OC-12)
- DS-3 configuration

## 1.89.3 Syntax Description

| | |
|---|---|
| `ds1` | Specifies the channel type is unchannelized DS1 and enters configuration mode for an unchannelized DS1 channel. |
| `channelized-ds1` | Specifies the channel type is channelized DS1 and enters configuration mode for a channelized DS1 channel. |
| *slot* | The chassis slot number where the line card is installed. |
| *port* | The number of the port containing the DS1 channel. |

| | |
|---|---|
| ***ds3-channel-id*** | When the DS1 channel is multiplexed in a channelized DS3 channel, the ***ds3-channel-id*** specifies the ID of the DS3 channel.<br>If you specify the ID of an unchannelized DS3, your attempt to configure an DS1 channel is rejected with the following message: `Incompatible channel type for ds1 subchannel.`<br>If you specify a DS3 channel ID that has not been configured, then the DS3 channel is created under the following conditions:<br>• If the ***port*** ID is for a SONET port where mapping is **sts1**, then a channelized-DS3 is created.<br>• If the ***port*** ID is for a SDH port where mapping is **au4-tu3**, then a channelized-DS3 is created with its default options.<br>• If neither of the above two conditions exist, then the no DS3 channel is created, and the following error is displayed: `Could not create channelized-ds3 channel.` |
| ***ds1-channel-id*** | The ID of the DS1 channel you are configuring. The range of values depends on whether the DS1 channel is nested within a channelized DS3 channel or nested directly within a channelized OC-3 or OC-12 port:<br>• **1-84** for a channelized or unchannelized DS1 channel within an channelized OC-3 port<br>• **1-336** for a channelized or unchannelized DS1 channel within an channelized OC-12 port<br>• **1-28** for a channelized or unchannelized DS1 channel in a channelized DS3 channel<br>The following restrictions apply:<br>• If you attempt to configure a channel type that is not supported by the port's SONET/SDH mapping, your configuration is rejected, and a message similar to the following is displayed: `channelized-ds1 14/7:1 port type is not supported under au4-tu12 mapping.`<br>• If you attempt to configure a channel as a type that is not supported by the port's service type, your configuration is rejected with the following message: `Channel type is incompatible with the port's service type.`<br>• If you attempt to configure an unchannelized DS1 channel on a port configured for CESoPSN service, your configuration is rejected, with the following message: `Channel type is incompatible with CESoPSN.` |

### 1.89.4 Usage Guidelines

- In the context of this command, a DS3 channel refers to the PDH structure that is mapped into the SONET or SDH frame. This is in contrast to a DS1 channel, which can either be a PDH channel mapped into the SONET frame or it can be a PDH subchannel that is multiplexed into the DS3 channel.

- If the port identified by ***port*** is configured for POS service, and the channel type is **ds1** (unchannelized), POS related features (such as encapsulation type) can be configured on the channel.

- The *aug-mapping* and *channel-mapping* commands determine into which channelized ports, you can configure the DS1. See *Configuring Channelized Ports* for further information.

## 1.89.5 Default

No channels on the port and no service bindings to those channels.

## 1.89.6 Examples

In the following example, the `port ds1 2/1:2:1` command enters port configuration mode for the first DS1 subchannel (unchannelized) multiplexed in the second DS3 channel (channelized). The `port channelized-ds1 2/1:2:3` command enters port configuration mode for the third DS1 subchannel (channelized ) multiplexed in the second DS3 channel (channelized).

```
port channelized-stm1 2/1 pos
 no shutdown
 aug-mapping au3-no-tug
 clock-source card-reference
 !
 port ds3 2/1:1
  no shutdown
  clock-source card-reference
  encapsulation ppp
  bind interface pos_chstm1->ds3_1 redkite1
 !
 port channelized-ds3 2/1:2
  no shutdown
  clock-source card-reference
 !
  port ds1 2/1:2:1
   no shutdown
   clock-source card-reference
   encapsulation ppp
   bind interface pos_chstm1->chds3->ds1_1 redkite1
  !
  port ds1 2/1:2:2
   no shutdown
   clock-source card-reference
   bind interface pos_chstm1->chds3->ds1_2 redkite1
  !
  !
  port channelized-ds1 2/1:2:3
   no shutdown
   clock-source card-reference
  !
   port ds0s 2/1:2:3:1
    no shutdown
    timeslot 1-12
    encapsulation ppp
    bind interface pos_chstm1->chds3->chds1->ds0s_1 redkite1
   !
```

# 1.90 port {ds3 | channelized-ds3}

**port {ds3 | channelized-ds3}** *slot/port:ds3-channel-id*

**no port {ds3 | channelized-ds3}** *slot/port*

## 1.90.1 Purpose

Enters the configuration mode for a DS3 channel in a channelized STM-1, STM-4, OC-3, or OC-12 port.

## 1.90.2 Command Mode

- Global Configuration

  Since the DS3 is configured in a channelized OC-3, OC-12, STM-1, or STM-4, you can also enter this command from the following modes:

- port configuration (OC-3)
- port configuration (OC-12)
- STM-1 configuration
- STM-4 configuration

## 1.90.3 Syntax Description

| | |
|---|---|
| **ds3** | Enters configuration mode for an unchannelized DS3 channel in a channelized OC-3, OC-12, STM-1, or STM-4 port.<br>The channel type is unchannelized DS3. |
| **channelized-ds3** | Enters configuration mode for an channelized DS3 channel in a channelized OC-3, OC-12, STM-1, or STM-4 port. The channel-type is channelized DS3.<br>The channel type is channelized DS3. |
| *slot* | Chassis slot number where the line card is installed. |

| | |
|---|---|
| ***port*** | Number of the port containing the DS3 channel. |
| ***ds3-channel-id*** | The channel ID of the DS3 channel you are configuring in a channelized OC-3, STM-1, OC-12, or STM-4 port:<br>• **`1-3`** for a channelized or unchannelized DS3 channel within a channelized OC-3 or STM-1 port.<br>• **`1-12`** for a channelized or unchannelized DS3 channel within an channelized OC-12 or STM-4 port<br>The following restrictions apply:<br>• If you attempt to configure a channel type that is not supported for the port's SONET/SDH mapping, your configuration is rejected, and a message similar to the following is displayed: `channelized-ds3 14/7:1 port type is not supported under au4-tu12 mapping`<br>• If you attempt to configure a channel as a type that is not supported by the port's service type, your configuration is rejected with the following message: `Channel type is incompatible with the port's service type.` |

## 1.90.4 Usage Guidelines

- In the context of this command, a DS3 channel refers to the PDH structure that is mapped into the SONET or SDH frame.
- If the port identified by ***port*** is configured for POS service, and the channel type is **`ds3`** (unchannelized), POS related features (such as encapsulation type) can be configured on the channel.
- The *aug-mapping* and *channel-mapping* commands determine into which channelized ports, you can configure the DS3. See *Configuring Channelized Ports* for further information.

## 1.90.5 Default

No channels on the port and no service bindings to those channels.

## 1.90.6 Examples

In the following example, the `port ds3 2/1:1` command enters port configuration mode for the first DS3 channel (unchannelized) in the STM-1 frame. The `channelized-ds3 2/1:2` command enters port configuration mode for the second DS3 channel (channelized) in the STM-1 frame.

```
port channelized-stm1 2/1 pos
 no shutdown
 aug-mapping au3-no-tug
 clock-source card-reference
 !
 port ds3 2/1:1
  no shutdown
  clock-source card-reference
  encapsulation ppp
  bind interface pos_chstm1->ds3_1 redkite1
 !
 port channelized-ds3 2/1:2
  no shutdown
  clock-source card-reference
 !
  port ds1 2/1:2:1
   no shutdown
   clock-source card-reference
   encapsulation ppp
   bind interface pos_chstm1->chds3->ds1_1 redkite1
  !
  port ds1 2/1:2:2
   no shutdown
   clock-source card-reference
   bind interface pos_chstm1->chds3->ds1_2 redkite1
  !
```

# 1.91 port {e1 | channelized-e1}

- To configure an E1 channel in a channelized STM-1 or STM-4 port:

  ```
  port {e1 | channelized-e1} slot/port:e1-channel-id
  ```

- To remove the E1 channel configurations in a channelized STM-1 or STM-4 port:

  ```
  no port port {e1 | channelized-e1} slot/port:ds3-channel
  -id
  ```

- To configure an E1 channel within a channelized DS3 channel:

  ```
  port {e1 | channelized-e1} slot/port:ds3-channel-id:e1-c
  hannel-id
  ```

- To remove the E1 subchannel configurations in a channelized DS3 channel:

  ```
  no port port {e1 | channelized-e1} slot/port:ds3-channel
  -id
  ```

## 1.91.1 Purpose

Enters the configuration mode for an E1 channel in a channelized STM-1 or STM-4 port, or in a channelized DS3 channel.

## 1.91.2 Command Mode

- Global Configuration

  Since the E1 is configured in a channelized STM-1, STM-4, or DS3, you can also enter this command from the following modes:

- STM-1 configuration
- STM-4 configuration
- DS-3 configuration

## 1.91.3 Syntax Description

| | |
|---|---|
| `e1` | Specifies the channel type is unchannelized E1 and enters configuration mode for an unchannelized E1 channel. |
| `channelized-e1` | Specifies the channel type is u1channelized E1 and enters configuration mode for an channelized E1 channel. |
| *`slot`* | The chassis slot number where the line card is installed. |
| *`port`* | The number of the port containing the E1 channel. |

| | |
|---|---|
| ***ds3-channel-id*** | When the E1 channel is multiplexed in a channelized DS3 channel, the ***ds3-channel-id*** specifies the ID of the DS3 channel.<br>If you specify the ID of an unchanneled DS3, your attempt to configure an E1 channel is rejected with the following message: `Incompatible channel type for e1 subchannel.`<br>If you specify a DS3 channel ID that has not been configured, then the DS3 channel is created under the following conditions:<br>• If the ***port*** ID is for a SONET port where mapping is **sts1**, then a channelized-DS3 is created.<br>• If the ***port*** ID is for a SDH port where mapping is **au4-tu3**, then a channelized-DS3 is created with its default options.<br>• If neither of the above two conditions exist, then the no DS3 channel is created, and the following error is displayed: `Could not create channelized-ds3 channel.` |
| ***e1-channel-id*** | The ID of the E1 channel you are configuring. The range of values depends on whether the E1 channel is nested within a channelized DS3 channel or nested directly within a channelized STM-1 or STM-4 port:<br>• `1-21` for an channelized or unchannelized E1 channel nested in a channelized DS3 channel<br>• `1-63` for a channelized or unchannelized E1 channel nested directly within an channelized STM-1 port<br>• `1-252` for a channelized or unchannelized E1 channel nested directly within an channelized STM-4 port<br>The following restrictions apply:<br>• If you attempt to configure a channel type that is not supported by the port's SONET/SDH mapping, your configuration is rejected, and a message similar to the following is displayed: `channelized-e1 14/7:1 port type is not supported under au4-tu12 mapping`<br>• If you attempt to configure a channel as a type that is not supported by the port's service type, your configuration is rejected with the following message: `Channel type is incompatible with the port's service type.` |

## 1.91.4 Usage Guidelines

- In the context of this command, a DS3 channel refers to the PDH structure that is mapped into the SONET or SDH frame. This is in contrast to an E1 channel, which can either be a PDH channel mapped into the SDH frame or it can be a PDH subchannel that is multiplexed into the DS3 channel.
- If the port identified by ***port*** is configured for POS service, and the channel type is **e1** (unchannelized), POS related features (such as encapsulation type) can be configured on the channel.
- The *aug-mapping* and *channel-mapping* commands determine into which channelized ports, you can configure the E1. See *Configuring Channelized Ports* for further information.

## 1.91.5 Default

No channels on the port and no service bindings to those channels.

### 1.91.6 Examples

In the following example, the `port e1 2/1:3:1` command enters port configuration mode for the first E1 subchannel (unchannelized) multiplexed into the third DS3 channel (channelized). The `port channelized-e1 2/1:3:3` command enters port configuration mode for the third E1 subchannel (channelized) multiplexed in the third DS3 channel (channelized).

```
port channelized-stm1 2/1 pos
 no shutdown
 aug-mapping au3-no-tug
 clock-source card-reference
 !
 port channelized-ds3 2/1:3
  no shutdown
  clock-source card-reference
 !
  port e1 2/1:3:1
   no shutdown
   clock-source card-reference
   encapsulation ppp
   bind interface pos_chstm1->chds3->e1_1 redkite1
  !
  port e1 2/1:3:2
   no shutdown
   clock-source card-reference
   bind interface pos_chstm1->chds3->e1_2 redkite1
  !
  port channelized-e1 2/1:3:3
   no shutdown
   clock-source card-reference
  !
   port ds0s 2/1:3:3:1
    no shutdown
    timeslot 1-15
    encapsulation ppp
    bind interface pos_chstm1->chds3->che1->ds0s_1 redkite1
   !
   port ds0s 2/1:3:3:16
    no shutdown
    timeslot 16-31
    bind interface pos_chstm1->chds3->che1->ds0s_2 redkite1
   !
  !
 !
!
!
```

# 1.92 port ethernet

**port ethernet** ***slot/port*** **[wan-phy]**

**no port ethernet** ***slot/port*** **[wan-phy]**

## 1.92.1 Purpose

Selects an Ethernet port and enters port configuration mode.

## 1.92.2 Command Mode

global configuration

## 1.92.3 Syntax Description

| | |
|---|---|
| *slot* | Chassis slot number of the line or controller card. The range of values depends on the chassis in which the line or controller card is installed; see the *card* command. |
| *port* | Line or controller card port number. The range of values depends on the type of line or controller card; see Table 30 of this command. |
| **wan-phy** | Enables WAN-PHY operation. A WAN-PHY port can transmit and receive IEEE 802.3 MAC frames directly in the payload envelope of a SONET STS-192c/SDH VC-4-64c frame. WIS is described in IEEE 802.3ae.<br>WAN-PHY is supported only on the 1-Port 10 Gigabit Ethernet Card (10ge-1-port ) and 1-Port 10 Gigabit Ethernet/OC-192c DDR (10ge-oc192-1-port). The Ethernet port on this card operates in either LAN-PHY or WHY-PHY mode. If you do not enter the `wan-phy` keyword, the port operates in LAN-PHY mode. (1) |

*(1) To change the configuration of the port of this card from LAN-PHY to WHY-PHY or from WHY-PHY to LAN-PHY, you must first delete the existing configuration.*

## 1.92.4 Default

None

## 1.92.5 Usage Guidelines

Use the **port ethernet** command to select an Ethernet port and enter port configuration mode. The Ethernet port can be of any type, including Gigabit Ethernet ports and the Ethernet management port on the active controller card.

**Note:** To change the configuration of the port of a 1-Port 10 Gigabit Ethernet Card (10ge-1-port ) and 1-Port 10 Gigabit Ethernet/OC-192c DDR (10ge-oc192-1-port) card from LAN-PHY to WHY-PHY or from WHY-PHY to LAN-PHY, you must first delete the existing configuration. For example, if the port is configured for WAN-PHY, enter the `no port ethernet` *`slot/port`* `wan-phy` command, which deletes WAN-PHY operation, then enter the command `port ethernet` *`slot/port`* to enable LAN-PHY.

For Ethernet management ports, the ***`slot`*** argument is always 1 in a SmartEdge 100 chassis, 6 in a SmartEdge 400 chassis, and 7 in a SmartEdge 600, 800, 1200, or 1200H chassis; the ***`port`*** argument is always 1.

**Note:** The SmartEdge 100 router limits the value of the ***`slot`*** argument to 2 for native ports and MIC ports.

Table 30 lists the range of values for the ***`port`*** argument for SmartEdge 400, 600, 800, 1200 and 1200H line cards.

*Table 30 Port Ranges for Ethernet Line Cards*

| Line Card Type | Physical Ports | Low-Density Version | Low-Density Ports |
|---|---|---|---|
| 10/100 Ethernet | 12 | No | – |
| Fast Ethernet-Gigabit Ethernet | 62[1] | No | – |
| Gigabit Ethernet | 4 | Yes | 1, 3 |
| Advanced Gigabit Ethernet | 4 | Yes | 1, 3 |
| Gigabit Ethernet 3 | 4 | No | – |
| Gigabit Ethernet 1020 | 10 | No | – |
| Gigabit Ethernet 1020 | 20 | No | – |
| Gigabit Ethernet | 5 | No | – |
| Gigabit Ethernet | 20 | No | – |
| Gigabit Ethernet DDR | 10 | No | – |
| 10 Gigabit Ethernet | 1 | No | – |
| 10 Gigabit Ethernet | 4 | No | – |
| 10 Gigabit Ethernet/OC-192c DDR | 1 | No | – |

*[1] On the FE-GE card, ports 1 to 60 are Fast Ethernet, while ports 61 and 62 are Gigabit Ethernet.*

**Note:**

The value for the ***port*** argument on the SmartEdge 100 router is either of the following:

- For a native port, it is 1 or 2.
- For a MIC port, it depends on the MIC and MIC slot in which it is installed.

Before the port is configured, the operating system performs a power check to determine if the SmartEdge router has sufficient unallocated power to meet the power requirements for the port's line card. If the power requirements for the line card are greater than the unallocated power resources of the chassis, the operating system displays the following message:

```
Insufficient power available for card <card-name> in slot <slot>.
Power Required: <n> A @48V Power Available: <m> A @48V
```

In the message, ***n*** is the amperes required by the line card and ***m*** is the amperes available for assignment. In this case, the command is not included in the system configuration. However, it might be possible to configure a line card that requires less power in this slot. Use the **show chassis power** command with the **inventory** keyword to display the power requirements for each line card.

To enable the port, use the **no shutdown** command in port configuration mode.

**Note:** If the system has dual controller cards installed, it is sufficient to configure the Ethernet management port on the controller card (slot 7 for SmartEdge 600, 800, 1200, 1200H chassis, or slot 6 for SmartEdge 400 chassis), depending on the chassis. Access to the system is switched to the standby controller card if it should become the active controller card during normal operations. Only the management port on the active controller card is enabled.

Use the **no** form of this command to delete the port configuration from the configuration database.

### 1.92.6 Examples

The following example shows how to configure an Ethernet port on the Ethernet line card installed in slot **2:**

```
[local]Redback(config)#port ethernet 2/2
[local]Redback(config-port)#no shutdown
```

# 1.93 port (http)

```
port [80]  [port-number]
```

## 1.93.1 Purpose

Selects the port or ports on which the HTTP server on the controller card listens.

## 1.93.2 Command Mode

HTTP redirect server configuration

## 1.93.3 Syntax Description

| | |
|---|---|
| `80` | Optional. Configures the HTTP server to listen on port 80. This is the default port. |
| *`port-number`* | Optional. Configures the HTTP server to listen to the specified port or ports. The supported ports range from 1025 to 51000. |

## 1.93.4 Default

The HTTP server listens on port 80.

## 1.93.5 Usage Guidelines

Use the **`port (http)`** command to select the port (or ports) on which the HTTP server on the controller card listens.

By default, the HTTP server listens on port 80. You can configure the HTTP server to listen on any port or ports (up to 10) ranging from 1025 to 51000. Including port 80, the total number of ports to which the HTTP server can listen is 11.

## 1.93.6 Examples

The following example configures the HTTP server to listen on ports **80**, **8080**, **1025**, **45000**, and **5000**:

```
[local]Redback(config)#http-redirect server
[local]Redback(config-hr-server)#port 80 8080  1025 45000 50000
```

# 1.94 port-limit

```
port-limit max-sessions
```

```
no port-limit
```

## 1.94.1 Purpose

Limits the number of sessions a subscriber can access simultaneously.

## 1.94.2 Command Mode

subscriber configuration

## 1.94.3 Syntax Description

| | |
|---|---|
| *max-sessions* | Maximum number of simultaneous subscriber sessions allowed. The range of values is 1 to 255. |

## 1.94.4 Default

There are no session limits.

## 1.94.5 Usage Guidelines

Use the **port-limit** command to limit the number of sessions a subscriber can access simultaneously. This command is useful for dial-up and ISDN users who might attempt to consume multiple links in their multilink bundle. You can also use this command to prevent a single user's account from being accessed by multiple users.

At runtime, if the subscriber sessions are using links in a Point-to-Point Protocol (PPP) multilink bundle, the maximum number of sessions (links) is reduced to eight if the value specified for the *max-sessions* argument is greater than eight. However, the value stored in the subscriber record is unchanged.

To set the port limit remotely using Remote Authentication Dial-In User Service (RADIUS), use the Port-Limit RADIUS attribute described in *RADIUS Attributes*.

Use the **no** form of this command to remove the session limitation.

### 1.94.6 Examples

The following example sets a maximum of two sessions for subscriber **joe** to use simultaneously:

```
[local]Redback(config-ctx)#subscriber name joe
[local]Redback(config-sub)#port-limit 2
```

# 1.95 port <port-type>

**port** ***port-type slot/port service-type***

**no port** ***port-type slot/port service-type***

## 1.95.1 Purpose

Configures a port on the *Channelized OC-3/STM-1 or OC-12/STM-4* line card for channelized OC-3, OC-12, STM-1, or STM-4 operation and enters the configuration mode of that port.

## 1.95.2 Command Mode

global configuration

## 1.95.3 Syntax Description

| | |
|---|---|
| *port-type* | • **channelized-oc3**<br>Framing: SONET, Line Rate=155.52 Mbps<br>• **channelized-oc12**<br>Valid for ports 1 and 5 only. Framing: SONET, Line Rate=622.08 Mbps.<br>• **channelized-stm1**<br>Framing: SDH, Line Rate=155.52 Mbps<br>• **channelized-stm4**<br>Valid for ports 1 and 5 only. Framing: SDH, Line Rate=622.08 Mbps |
| *slot* | Chassis slot number of the line card. |
| *port* | Line card port number. |
| *service-type* | The service type attribute determines the function of a port and governs lower-level port and channel configurations.<br>• **pos** (Packet over SONET)<br>• **ces** (Circuit Emulation Services) |

## 1.95.4 Usage Guidelines

Configures a port on the *Channelized OC-3/STM-1 or OC-12/STM-4* line card for channelized OC-3, OC-12, STM-1, or STM-4 operation and enters the configuration mode of that port.

- To change port framing type, you must first unconfigured all ports.
- All ports on a card must be SONET or SDH. A combination of SONET and SDH is not supported.

  Attempts to configure card ports for SDH once it has SONET ports configured, or to configure card ports for SONET once it has SDH ports configured is rejected, with the following messages displayed:

```
mix SONET/SDH ports not allowed
```

- An "all-ports" software license is required for ports 5 - 8. See the *all-ports* command for details.

  An attempt to configure port-ids in the range 5-8 is rejected if the all-ports software license is not in place for the specified ***slot***, and the following message is displayed:

  ```
  all-ports software license required
  ```

- If port 1 is configured for channelized-oc12, or channelized-stm4, then attempts to configure ports 2 through 4 are rejected with the following error message displayed:

  ```
  channelized-oc12 14/1 port already set as different
  variant.
  ```

  ```
  channelized-stm4 14/1 port already set as different
  variant.
  ```

- If port 5 is configured for channelized-oc12, or channelized-stm4, then attempts to configure ports 6 through 8 are rejected, with the following error message displayed:

  ```
  channelized-oc12 14/5 port already set as different
  variant.
  ```

  ```
  channelized-stm4 14/5 port already set as different
  variant.
  ```

- If ports 2 through 4 are configured, then an attempt to configure port 1 as channelized-oc12 or channelized-stm4 is rejected, with the following message displayed:

  ```
  channelized-oc3 14/2 port has already occupied port
  group 1-4.
  ```

  ```
  channelized-stm1 14/2 port has already occupied port
  group 1-4.
  ```

- If ports 6 through 8 are configured, then an attempt to configure port 5 as channelized-oc12, or channelized-stm4, is rejected with the following message displayed:

  ```
  channelized-oc3 14/7 port has already occupied port
  group 5-8.
  ```

  ```
  channelized-stm1 14/7 port has already occupied port
  group 5-8.
  ```

- The **no** form of this command removes the port framing and all configured channels on the specified port.

### 1.95.5 Default

No configured channels on the port and no service bindings to those channels.

### 1.95.6 Examples

In the following example, the `port channelized-stm1 2/1 pos` command sets the service type to POS and enters channelized STM-1 port configuration mode.

```
port channelized-stm1 2/1 pos
 no shutdown
 aug-mapping au3-no-tug
 clock-source card-reference
 !
 port ds3 2/1:1
  no shutdown
  clock-source card-reference
  encapsulation ppp
  bind interface pos_chstm1->ds3_1 redkite1
 !
 port channelized-ds3 2/1:2
  no shutdown
  clock-source card-reference
 !
  port ds1 2/1:2:1
   no shutdown
   clock-source card-reference
   encapsulation ppp
   bind interface pos_chstm1->chds3->ds1_1 redkite1
  !
  port ds1 2/1:2:2
   no shutdown
   clock-source card-reference
   bind interface pos_chstm1->chds3->ds1_2 redkite1
  !
```

# 1.96 port pos

```
port pos slot/port

no port pos slot/port
```

## 1.96.1 Purpose

Configures a Packet over SONET/SDH (POS) port and enters port configuration mode.

## 1.96.2 Command Mode

global configuration

## 1.96.3 Syntax Description

| | |
|---|---|
| *slot* | Chassis slot number of the line card. The range of values depends on the chassis in which the line card is installed; see the Line and Services Card Types and Slots section in the *Usage Guidelines* of the *card* command. |
| *port* | Line card port number. The range of values depends on the type of line card; see Table 31 of this command. |

## 1.96.4 Default

None

## 1.96.5 Usage Guidelines

Use the **port pos** command to configure a POS port on an OC-48c/STM-16 line card, and to enter port configuration mode.

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

Table 31 lists the range of values for the *port* argument.

*Table 31 Port Ranges for POS Line Cards*

| Line Card Type | Physical Ports | Low-Density Version | Low-Density Ports |
|---|---|---|---|
| OC-192c/STM-64c | 1 | No | – |
| OC-48c/STM-16c | 4 | No | – |

Before the port is configured, the SmartEdge OS performs a power check to determine if the chassis has sufficient unallocated power to meet the power requirements for the port's line card. If the power requirements for the line card are greater than the unallocated power resources of the chassis, the SmartEdge OS displays the following message:

```
Insufficient power available for card <card-name> in slot <slot>.
Power Required: <n> A @48V Power Available: <m> A @48V
```

In the message, ***n*** is the amperes required by the line card and ***m*** is the amperes available for assignment. In this case, the command is not included in the system configuration. However, it might be possible to configure a line card that requires less power in this slot. Use the **show chassis power** command with the **inventory** keyword to display the power requirements for each line card.

To enable the port, use the **no shutdown** command in port configuration mode.

Use the **no** form of this command to delete the port configuration from the configuration database.

### 1.96.6 Examples

The following example shows how to configure an POS port on the OC card installed in slot **6:**

```
[local]Redback(config)#port pos 6/1
[local]Redback(config-port)#no shutdown
```

# 1.97 port-priority

**port-priority** ***priority-value***

{**no** | **default**} **port-priority**

## 1.97.1 Purpose

Sets the Rapid Spanning Tree Protocol (RSTP) priority of the associated port.

## 1.97.2 Command Mode

- spanning-tree profile configuration

## 1.97.3 Syntax Description

| | |
|---|---|
| ***priority-value*** | RSTP port priority. The range of values is from 0 to 240. Only multiples of 16 are allowed as values for the argument. |

## 1.97.4 Default

The default RSTP priority is 16.

## 1.97.5 Usage Guidelines

Use the **port-priority** command to set the RSTP priority of the associated port. If multiple ports have the same path cost to the root bridge, the port with lowest port priority is selected as the root port.

## 1.97.6 Examples

The following example illustrates how the **spanning-tree profile** command creates the spanning-tree profile **womp** and sets its port priority to the value **224**. In the second part of the example, an Ethernet port is assigned the spanning-tree profile **womp** and, therefore, the priority of the Ethernet port is set at **224:**

```
[local]Redback(config)#spanning-tree profile womp
[local]Redback(config-stp-prof)#port-priority 224
[local]Redback(config-stp-prof)#exit
[local]Redback(config)#port ethernet 1/1
[local]Redback(config-port)#spanning-tree profile womp
```

## 1.98 port-propagate qos from ethernet

**port-propagate qos from ethernet** [**class-map** ***map-name***]

{**no** | **default**} **port-propagate qos from ethernet** [**class-map** ***map-name***]

### 1.98.1 Purpose

For incoming packets, enables the use of 802.1p user priority bits in the 802.1q Ethernet header to set the internal SmartEdge packet descriptor (PD) quality of service (QoS) bits for the packet and determine ingress oversubscription treatment.

### 1.98.2 Command Mode

Port configuration for cards that support differentiated packet treatment for ingress oversubscription scenarios.

### 1.98.3 Syntax Description

| | |
|---|---|
| **class-map** ***map-name*** | Optional. Name of an ingress Ethernet classification map for mapping Ethernet 802.1p user priority bits to quality of service (QoS) packet descriptor (PD) values. |

### 1.98.4 Default

Ethernet 802.1p user priority bits are not propagated to PD QoS bits or used to determine ingress oversubscription treatment.

### 1.98.5 Usage Guidelines

Use the **port-propagate qos from ethernet** command to propagate Ethernet 802.1p user priority bits to PD QoS bits for incoming packets. Use the 802.1p value in the outer 802.1q header, if present, of each received packet to determine its ingress oversubscription treatment. For more information, see *Priority Propagation for Oversubscribed Traffic Cards* .

**Note:** This command applies to all incoming packets transmitted over 802.1Q permanent virtual circuits (PVCs) that are received on the port.

Use the **qos class-map** command with the ethernet in keywords (in global configuration mode) to define an optional custom mapping schema to be referenced by the **class-map** ***map-name*** option of the **port-propagate qos from ethernet** command. The **ethernet use-ip** class-map command is not supported in this context and should not be configured in class-maps which are to be used with this command.

If no class-map is specified with the **`port-propagate qos from ethernet`** command, the PD QoS priority value is mapped directly from the 802.1p value of the packet according to the mapping specified in Table 32.

*Table 32 Mapping of PD QoS Priority Value to 802.1p Value without class-map Specified*

| 802.1p Value | PD QoS Priority Value | PD QoS Drop-precedence Value |
|---|---|---|
| 7 | 0 | 0 |
| 6 | 1 | 0 |
| 5 | 2 | 0 |
| 4 | 3 | 0 |
| 3 | 4 | 0 |
| 2 | 5 | 0 |
| 1 | 6 | 0 |
| 0 | 7 | 0 |

Use the **`no`** or **`default`** form of this command to disable the propagation of Ethernet 802.1p bits to PD QoS bits and use of 802.1p to determine ingress oversubscription treatment.

For more information about port propagation, see *Priority Propagation for Oversubscribed Traffic Cards*.

### 1.98.6 Examples

The following example shows how to propagate Ethernet 802.1p user priority bits to PD QoS bits and use the 802.1p bits to determine ingress oversubscription treatment for incoming packets arriving in slot 2, port 1 of an ethernet port:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#port-propagate qos from ethernet
```

# 1.99 port-propagate qos from ip

**port-propagate qos from ip** [**class-map** ***map-name***]

{**no** | **default**} **port-propagate qos from ip** [**class-map** ***map-name***]

## 1.99.1 Purpose

For incoming packets, enable use of Differentiated Services Code Point (DSCP) bits in the IP packet header to set the internal SmartEdge packet descriptor (PD) quality of service (QoS) bits for the packet and determine ingress oversubscription treatment.

## 1.99.2 Command Mode

Port configuration for cards that support differentiated packet treatment for ingress oversubscription scenarios.

## 1.99.3 Syntax Description

| | |
|---|---|
| **class-map** ***map-name*** | Optional. Name of the schema for mapping DSCP bits to PD priority bits. |

## 1.99.4 Default

IP DSCP bits are not propagated to PD QoS bits or used to determine ingress oversubscription treatment.

## 1.99.5 Usage Guidelines

Use the **port-propagate qos from ip** command to propagate IP DSCP user priority bits to PD QoS bits and use the DSCP value in the IP header, if present, of each received packet to determine its ingress oversubscription treatment. For more information, see *Priority Propagation for Oversubscribed Traffic Cards* .

Use the **qos class-map** command with the **ip in** keywords (in global configuration mode) to define an optional custom mapping schema to be referenced by the **port-propagate qos from ip** command.

If no class-map is specified with the **class-map** ***map-name*** option of the **port-propagate qos from ip** command, the PD QoS priority value is mapped directly from the IP DSCP value of the packet according to the mapping specified in Table 33.

*Table 33 Mapping of PD QoS Priority Value to IP DSCP Value without class-map Specified*

| IP DSCP Value | PD QoS Priority Value | PD QoS Drop-precedence Value |
|---|---|---|
| 111xxxb | 0 | 0 |
| 110xxxb | 1 | 0 |
| 101xxxb | 2 | 0 |
| 100xxxb | 3 | 0 |
| 011xxxb | 4 | 0 |
| 010xxxb | 5 | 0 |
| 001xxxb | 6 | 0 |
| 000xxxb | 7 | 0 |

When the **port-propagate** command is used to map IP DSCP values to PD QoS values, only the three most significant bits (the DSCP class-selector or precedence) are relevant, and the three least significant bits (DSCP drop-precedence) are ignored and treated as if they were zero. Therefore, in IP class-maps referenced by the **port-propagate** command, only the entries for which the “ip” value is evenly divisible by "8" are relevant.

For example, in the following class-map:

```
qos class-map port_in ip in
ip 8 to qos 11
ip 9 to qos 12
```

The `ip 8 entry is used for all packets in assured forwarding class "1", and the ip 9 value is never used because the three least significant bits are non-zero. For convenience, use the "csN" DSCP labels when defining class-map entries for use with the` **port-propagate** command:

```
qos class-map port_in ip in
ip cs1 to qos 11
ip cs2 to qos 19
```

Use the **no** or **default** form of this command to disable propagation of IP DSCP to PD QoS and use of IP DSCP to determine ingress oversubscription treatment.

### 1.99.6 Examples

The following example shows how to propagate DSCP bits in the IP packet header to the PD priority bits and use DSCP bits to determine ingress oversubscription treatment for incoming packets arriving in slot 2, port 2 of an ethernet port:

```
[local]Redback(config)#port ethernet 2/2
[local]Redback(config-port)#port-propagate qos from ip
```

# 1.100 port-propagate qos from mpls

**`port-propagate qos from mpls`** [**`class-map`** ***`map-name`***]

{**`no`** | **`default`**} **`port-propagate qos from mpls`** [**`class-map`** ***`map-name`***]

## 1.100.1 Purpose

For incoming packets, enable use of MPLS experimental (EXP) bits to set the internal SmartEdge packet descriptor (PD) quality of service (QoS) bits for the packet and determine ingress oversubscription treatment.

## 1.100.2 Command Mode

Port configuration for cards that support differentiated packet treatment for ingress oversubscription scenarios.

## 1.100.3 Syntax Description

| | |
|---|---|
| **`class-map`** ***`map-name`*** | Optional. Name of the ingress MPLS classification map for mapping MPLS EXP values to QoS PD values. |

## 1.100.4 Default

MPLS EXP bits are not mapped to PD QoS bits or used to determine ingress oversubscription treatment.

## 1.100.5 Usage Guidelines

Use the **`port-propagate qos from mpls`** command to enable mapping MPLS EXP bits to PD QoS values for incoming packets and use each received EXP value of the packet in the MPLS header, if present, to determine its ingress oversubscription treatment. For more information, see *Priority Propagation for Oversubscribed Traffic Cards* .

Use the **`qos class-map`** command with the **`mpls in`** keywords (in global configuration mode) to define an optional custom mapping schema to be referenced by the **`class-map`** ***`map-name`*** option of the **`port-propagate qos from mpls`** command. The **`mpls use-ethernet`** and **`mpls use-ip`** class-map commands are not supported in this context and should not be configured in class-maps which are to be used with the **`port-propagate qos from mpls`** command.

If no class-map is specified with the **`port-propagate qos from mpls`** command, the PD QoS priority value is mapped directly from the EXP value of the packet according to the mapping specified in Table 34.

*Table 34 Mapping of PD QoS Priority Value to EXP Value without class-map Specified*

| EXP Value | PD QoS Priority Value | PD QoS Drop-precedence Value |
|---|---|---|
| 7 | 0 | 0 |
| 6 | 1 | 0 |
| 5 | 2 | 0 |
| 4 | 3 | 0 |
| 3 | 4 | 0 |
| 2 | 5 | 0 |
| 1 | 6 | 0 |
| 0 | 7 | 0 |

Use the **no** or **default** form of this command to disable the mapping of MPLS EXP bits to PD QoS bits and use of EXP to determine ingress oversubscription treatment.

### 1.100.6 Examples

The following example shows how to propagate MPLS EXP bits to PD QoS bits and use EXP bits to determine ingress oversubscription treatment for incoming packets arriving in slot 2, port 2 of an ethernet port:

```
[local]Redback(config)#port ethernet 2/2
[local]Redback(config-port)#port-propagate qos from mpls
```

# 1.101 port pseudowire

**port pseudowire** ***pw_name***

**no port pseudowire** ***pw_name***

## 1.101.1 Command Mode

global configuration

## 1.101.2 Syntax Description

| | |
|---|---|
| *pw_name* | Port pseudowire connection name. |

## 1.101.3 Default

none

## 1.101.4 Usage Guidelines

Use the **port pseudowire** command to configure a port PW connection and enter port configuration mode to add attributes to the port PW.

You can configure up to 250 port PWs per router.

Use the **no** form of this command to disable a port PW connection.

## 1.101.5 Examples

The following example shows how to configure a port PW Ethernet connection called **connect1:**

```
[local]Redback(config)#port pseudowire connect1
```

# 1.102 port (RFlow)

```
port destination-port

no port destination-port
```

## 1.102.1 Purpose

Configures access to a port on an external collector. This is the port on which you want the external collector to receive exported records.

## 1.102.2 Command Mode

flow collector configuration

## 1.102.3 Syntax Description

| | |
|---|---|
| *destination-port* | Identifies a port on an external collector that listens for flow records that are exported from the SmartEdge router. Range is from 1 through 16384. |

## 1.102.4 Default

The default destination port for a collector is 9997.

## 1.102.5 Usage Guidelines

Use the `port` command in flow collector configuration mode to configure access to a port on an external collector. This is the port on which the external collector receives exported records.

Use the `no` form of this command to return the collector to using the default destination port 9997.

## 1.102.6 Examples

The following example shows how to configure access to the destination port **10** on the external collector **c1:**

```
[local]Redback#configure
[local]Redback(config)#context foo
[local]Redback(config-ctx)#flow collector c1
[local]Redback(config-flow-collector)#port 10
```