ERICSSON

Commands: dec through dz

COMMAND DESCRIPTION

7/190 82-CRA 119 1170/1-V1 Uen J

Contents

1 Command Descriptions

Commands starting with “dec” through commands starting with “dz” 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 decrement ttl

```
decrement ttl
```

```
no decrement ttl
```

1.1.1 Purpose

Enables transit routers to decrement the Multiprotocol Label Switching (MPLS) time-to-live (TTL) by 1 at each hop.

1.1.2 Command Mode

MPLS router configuration

1.1.3 Syntax Description

This command has no keywords or arguments.

1.1.4 Default

Transit routers are enabled to decrement the MPLS TTL by 1 at each hop.

1.1.5 Usage Guidelines

Use the **decrement ttl** command to enable transit routers to decrement the MPLS TTL by 1 at each hop.

Use the **no** form of this command to disable transit routers from decrementing the MPLS TTL by 1 at each hop.

Note: The default behavior of the SmartEdge router is to decrement the MPLS TTL by 1 at each hop, so the **decrement ttl** command is used to return the router to its default behavior after it has been changed by the **no** form of this command.

1.1.6 Examples

The following example shows how to enable transit routers to decrement the MPLS TTL by 1 at each hop:

```
[local]Redback(config-ctx)#router mpls 234
[local]Redback(config-mpls)#decrement ttl
```

1.2 default-information originate

default-information originate [**route-map** *map-name*]

{**no** | **default**} **default-information originate** [**route-map** *map-name*]

1.2.1 Purpose

In RIP or RIPng interface configuration mode, configures the specified Routing Information Protocol (RIP) or RIP next generation (RIPng) interface to originate the default route.

In RIP or RIPng router configuration mode, injects the default route into the RIP or RIPng instance.

1.2.2 Command Mode

- RIP interface configuration
- RIPng interface configuration
- RIPng router configuration
- RIP router configuration

1.2.3 Syntax Description

route-map *map-name*	Optional. Route map name. The conditions of the route map are applied to the default route.

1.2.4 Default

The default route is not sent.

1.2.5 Usage Guidelines

Use the **default-information originate** command (in RIP or RIPng interface configuration mode) to configure the specified RIP or RIPng interface to originate the default route, which is 0.0.0.0 for IPv4 and ::/0 for IPv6.

Use the **default-information originate** command (in RIP or RIPng router configuration mode) to inject the default route into the RIP or RIPng instance.

To apply a route map to the default route, use the optional **route-map** ***map-name*** construct. In this case, the default route is generated only when there is a match in the specified route map.

Use the **no** or **default** form of this command (in RIP or RIPng interface configuration mode) to configure the interface to not originate the default route.

Use the **no** or **default** form of this command (in RIP or RIPng router configuration mode) to not inject the default route into the RIP or RIPng instance.

1.2.6 Examples

The following example shows how to inject the default route into the **rip001** RIP instance:

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#default-information originate
```

The following example shows how to originate the default route from the **fe1** interface for the **rip002** RIP instance:

```
[local]Redback(config-ctx)#router rip rip002

[local]Redback(config-rip)#interface fe1

[local]Redback(config-rip-if)#default-information originate
```

1.3 default-lease-time

default-lease-time *seconds*

no default-lease-time

1.3.1 Purpose

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

1.3.2 Command Mode

- DHCP server configuration
- DHCP subnet configuration

1.3.3 Syntax Description

seconds	Length of time for the default lease. The range of values is 180 seconds 900 seconds (15 minutes) to 31,536,000 seconds (one year).

1.3.4 Default

The default length of time is two hours.

1.3.5 Usage Guidelines

Use the **default-lease-time** command to specify the default lease time for the DHCP server or one of its subnets. In DHCP server configuration mode, this command specifies the default lease time for all subnets; in DHCP subnet configuration mode, it specifies the default lease time for that subnet. The value you specify for a subnet overrides the global value for the server.

Note: If the default lease time is set very low, it will affect the performance of the SmartEdge router, causing some subscribers to lose their leases.

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

1.3.6 Examples

The following example shows how to specify a default lease time of 4 hours (**14000**) 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)#default-lease-time 14400
```

1.4 default-metric (OSPF)

default-metric ***metric***

no default-metric

1.4.1 Purpose

Configures the default metric used for redistributed Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) routes when no metric is specified.

1.4.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.4.3 Syntax Description

metric	Metric value. The range of values is 1 to 16,777,215.

1.4.4 Default

No default metric is configured. If a metric value is not configured through the **redistribute** command in OSPF router configuration mode or applied via a route map, the metric in the system routing table is used.

1.4.5 Usage Guidelines

Use the **default-metric** command to configure the default metric used for redistributed OSPF or OSPFv3 routes when no metric is specified. You can specify a metric through the **redistribute** command (in OSPF or OSPF3 router configuration mode), or indirectly by applying a route map through the **route-map** command (in route map configuration mode).

Use the **no** form of this command to return the metric value to its default setting.

1.4.6 Examples

The following example shows how to configure a default metric value of **40:**

```
[local]Redback(config-ospf)#default-metric 40
```

1.5 default-metric (RIP)

default-metric *metric*

{**no** | **default**} **default-metric**

1.5.1 Purpose

Sets the default metric for the Routing Information Protocol (RIP) or RIP next generation (RIPng) instance.

1.5.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.5.3 Syntax Description

metric	Default metric. The range of values is 0 to 16; the default value is 0.

1.5.4 Default

The metric value is 0.

1.5.5 Usage Guidelines

Use the **default-metric** command to set the default metric for the RIP or RIPng instance. The default value is used when a route with incompatible metrics is received into the RIP or RIPng instance; for example, when a route from a different routing domain is imported into RIP or RIPng.

Use the **no** or **default** form of this command to return the default metric value to 0.

1.5.6 Examples

The following example shows how to set the default metric to **11** for the RIP instance, **rip001:**

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#default-metric 11
```

1.6 default-originate

default-originate [**route-map** *map-name*]

no default-originate [**route-map** *map-name*]

1.6.1 Purpose

Advertises the default route of the specified address family, even when the default route is not installed in the Border Gateway Protocol (BGP) routing table, to the BGP neighbor.

1.6.2 Command Mode

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

1.6.3 Syntax Description

route-map *map-name*	Optional. Name of the route map. The match and set conditions of the specified route map are applied before the default route is sent.

1.6.4 Default

No default route is sent to peers.

1.6.5 Usage Guidelines

Use the **default-originate** command to advertise the default route of the specified address family, even when the default route is not installed in the BGP routing table, to the BGP neighbor. The default route, 0.0.0.0/0, is typically sent to a BGP neighbor that does not carry full Internet routes.

If the **route-map** *map-name* keyword construct is not used, or if the specified route map does not include a **match ip address prefix-list** *pl-name* statement, the specified address family unconditionally advertises the default route to the BGP neighbor.

When the **route-map** *map-name* keyword construct is used, and the route map has a **match ip address prefix-list** *pl-name* statement, the specified address family advertises the default route only if the address prefix entry specified in the IP prefix list exists in the routing information base (RIB).

Use the **no** form of this command to avoid sending the default route to neighbors or peer groups.

1.6.6 Examples

The following example shows how to send the unicast default route unconditionally to the neighbor at IP address **102.210.210.1**, and only send it to the neighbor at IP address, **68.68.68.68**, when route, **20.0.0.0/8**, with the next-hop address, **192.192.192.253:**

```
[local]Redback(config-ctx)#route-map map1
[local]Redback(config-route-map)#match ip address prefix-list pref1
[local]Redback(config-route-map)#match ip next-hop prefix-list next-hop-list
[local]Redback(config-route-map)#exit
[local]Redback(config-ctx)#ip prefix-list pref1
[local]Redback(config-prefix-list)#permit 20.0.0.0/8
[local]Redback(config-prefix-list)#exit
[local]Redback(config-ctx)#ip prefix-list next-hop-list
[local]Redback(config-prefix-list)#permit 192.192.192.253/32
[local]Redback(config-prefix-list)#exit
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#remote-as 200
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#default-originate
[local]Redback(config-bgp-peer-af)#exit
[local]Redback(config-bgp-neighbor)#exit
[local]Redback(config-bgp)#neighbor 68.68.68.68 external
[local]Redback(config-bgp-neighbor)#remote-as 300
[local]Redback(config-bgp-neighbor)#address-family ipv4 unicast
[local]Redback(config-bgp-peer-af)#default-originate route-map map1
```

1.7 default-peer

default-peer *peer-addr* [*pl-name*]

no default-peer *peer-addr* [*pl-name*]

1.7.1 Purpose

Configures a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source active (SA) messages.

1.7.2 Command Mode

MSDP router configuration

1.7.3 Syntax Description

peer-addr	Peer IP address to be set as the default peer.
pl-name	Optional. Name of the Border Gateway Protocol (BGP) prefix list which specifies that the peer will be a default peer only for the prefixes listed in the list. A BGP prefix list must be configured for this *pl-name* argument to have any effect.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **default-peer** command to configure a default peer from which to accept all MSDP SA messages. A default peer is needed in topologies where MSDP peers do not coexist with BGP peers. In such a case, the reverse path forwarding (RPF) check on SA messages can fail, and no SA messages are accepted. In these cases, you can configure the peer as a default peer, and bypass RPF checks.

Note: An MSDP peer must already be configured before it can be made a default peer.

The *peer-addr* argument must be the IP address of a previously configured peer.

Use the *pl-name* argument to allow only those SA entries whose RP is permitted in the prefix list; otherwise, all SA messages from the default peer are accepted.

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

1.7.6 Examples

The following example shows how to configure the peer address, **192.168.3.8**, as the default peer:

```
[local]Redback(config-ctx)#router msdp
[local]Redback(config-msdp)#default-peer 192.168.3.8
```

1.8 default-route

default-route [**metric** *metric*] [**metric-type** *type*]

no default-route

1.8.1 Purpose

Changes the attributes of a default route originated into a stub area or a not-so-stubby-area (NSSA).

1.8.2 Command Mode

- OSPF area configuration
- OSPF3 area configuration

1.8.3 Syntax Description

metric *metric*	Optional. Metric value for the default route. The range of values is 1 to 1,677,214; 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: • **1**—Specifies a Type 1 metric type. • **2**—Specifies a Type 2 metric type.

1.8.4 Default

The metric value for the default route is 1. For stub areas, a Type 3 LSA with a metric value of 1 is advertised and the metric type is ignored. For NSSAs that import summary advertisements, a Type 7 LSA with a metric value of 1 and a route metric type of 2 is advertised. For NSSAs that do not import summary advertisements, a Type 3 LSA with a metric value of 1 is advertised and the metric type is ignored.

1.8.5 Usage Guidelines

Use the **default-route** command to change the attributes of a default route originated into a stub area or NSSA. The LSA advertising the default route depends on the area type and whether summary advertisements (Type 3 and 4 LSAs) are advertised into the area.

For stub areas, a Type 3 LSA with a metric value of 1 is advertised by default. The **default-route** command can be used to modify the metric. The metric type is ignored.

For NSSAs that import summary advertisements, a Type 7 LSA with a metric value of 1 and route metric type of 2 is advertised by default. The **default-route** command can be used to modify the metric or metric type.

For NSSAs that do not import summary advertisements, a Type 3 LSA with a metric value of 1 is advertised by default. The **default-route** command can be used to modify the metric. The metric type is ignored.

If there are two routers originating a default route with the same metric value, the closest router is chosen to perform routing.

Use the **no** form of this command to restore the default attributes for the originated default route.

1.8.6 Examples

The following example shows how to configure a default route metric value of **3:**

```
[local]Redback(config-ospf-area)#default-route metric 3
```

1.9 delete

delete [**mate**] [**crashfile**] ***url*** [**-noconfirm**]

1.9.1 Purpose

Deletes a file from the local file system on either the active or standby controller card.

1.9.2 Command Mode

exec (10)

1.9.3 Syntax Description

mate	Optional. Specifies that the file to be deleted is on the controller card to which you are not connected.
crashfile	Optional. Specifies that the file to be deleted is a crash file.
url	URL of the file to be deleted.
-noconfirm	Optional. Deletes files without asking for confirmation.

1.9.4 Default

None

1.9.5 Usage Guidelines

Use the **delete** command to delete a file from the local file system on either the active or standby controller card.

Use the **mate** keyword to specify the controller card to which you are not connected.

Note: The SmartEdge 100 router does not support standby controller cards; therefore, the **mate** keyword is not applicable.

When referring to a file, the URL takes the following form:

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

The value for the ***device*** argument can be **flash**, or if a mass-storage device is installed, **md**. If you do not specify the ***device*** argument, the default value is the device in the current working directory. If you do not specify the ***directory***

argument, the default value is the current directory. Directories can be nested. The value for the ***filename*** argument can be up to 256 characters in length.

Use the command-line interface (CLI) online Help for this command or the **show crashfiles** command (in any mode) to list the crash files currently located on the system.

If you do not specify the **-noconfirm** keyword, the system prompts you to confirm the deletion. Enter **y** to confirm the operation; if you enter any other character, the system does not delete the file.

1.9.6 Examples

The following example shows how to delete a file in a nested subdirectory:

```
[local]Redback#delete /flash/backup/old/current.cfg
```

The following example shows how to delete a crash file using the online Help to determine the URL; a confirmation message is accepted:

```
[local]Redback#delete crashfile ?


  /md/dlmd_50.core

  /md/dlmd_50.mini.core

  WORD                    URL of file to delete in local filesystem


[local]Redback#delete crashfile /md/dlmd_50.core

Are you sure you want to delete /md/dlmd_50.core ?y
```

1.10 delete partition

delete partition sse *slot disk_num partition_name*

1.10.1 Command Mode

exec (10)

1.10.2 Syntax Description

sse *slot*	Chassis slot number of the SSE card.
disk_num	Disk number on the SSE card. Values: 1 or 2.
partition_name	Name of the partition.

1.10.3 Default

None.

1.10.4 Usage Guidelines

Removes the specified partition on an SSE disk.

All data in the partition is deleted.

This command cannot be executed if the partition is mounted on any other card.

1.10.5 Examples

The following example shows how to Remove a partition on an SSE disk:

```
[local]Redback#delete partition sse 2 1 p01
```

```
[local]Redback#delete partition sse 2 1 p01
```

1.11 demand-circuit

demand-circuit

no demand-circuit

1.11.1 Purpose

Configures Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) to treat a point-to-point (P2P) or point-to-multipoint (P2MP) interface as a demand circuit as described in RFC 1793, *Extending OSPF to Support Demand Circuits*.

1.11.2 Command Mode

- OSPF interface configuration
- OSPF3 interface configuration

1.11.3 Syntax Description

This command has no keywords or arguments.

1.11.4 Default

Demand circuit support is disabled on P2P and P2MP interfaces. Demand circuit support is implicitly enabled on virtual links and sham links.

1.11.5 Usage Guidelines

Use the **demand-circuit** command to configure OSPF or OSPFv3 to treat a P2P or P2MP interface as a demand circuit, as described in RFC 1793, *Extending OSPF to Support Demand Circuits*.

Demand circuits are network segments whose costs vary with usage; charges can be based both on connect time and on bytes or packets transmitted. OSPF or OSPFv3 routing usually requires a demand circuit's underlying data-link connection to be constantly open, resulting in unwanted usage charges. Using the **demand-circuit** command enables OSPF or OSPFv3 Hello packets and the refresh of OSPF or OSPFv3 routing information to be suppressed on-demand circuits, allowing the underlying data-link connections to be closed when not carrying traffic.

Note: Hello suppression is not be negotiated unless demand circuit support is enabled.

Use the **no** form of this command to remove the demand circuit designation.

1.11.6 Examples

The following example shows how to configure the OSPF interface **POS1/2** in area **0** to be a demand circuit:

```
[local]Redback(config-ospf)#area 0

[local]Redback(config-ospf-area)#interface POS1/2

[local]Redback(config-ospf-if)#demand-circuit
```

1.12 deny (IPv4 ACL)

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

deny [*protocol*] {*src src-wildcard* | **any** | **host** *src*} [*cond port* | **range** *port end-port*] [*dest dest-wildcard* | **any** | **host** *dest*] [*cond port* | **range** *port end-port*] [**length** {*cond length* | **range** *length end-length*}] [**icmp-type** *icmp-type* [**icmp-code** *icmp-code*]] [**igmp-type** *igmp-type*] [**dscp eq** *dscp-value*] [**established** | **setup** | **invalid-tcp-flags**] [**precedence** *prec-value*] [**tos** *tos-value*] [[**fragments**] | [**ip-options**]] [**condition** *cond-id*]

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

1.12.1 Purpose

Creates an IPv4 access control list (ACL) statement that denies packets that meet the specified criteria.

1.12.2 Command Mode

Access control list configuration

1.12.3 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 Table 1.
src	Source address to be included in the permit or deny criteria. An IP address in the form *A.B.C.D*.
src-wildcard	Indication of which bits in the *src* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Any zero-bits in the *src-wildcard* argument must be matched by the corresponding bits in the *src* argument. For any one-bits in the *src-wildcard* argument, the corresponding bits in the *src* argument are ignored.
any	Specifies a completely wildcard source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.
host *src*	Address of a single-host source with no wildcard address bits. The **host** *source* construct is identical to the *src src-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).

cond	Optional. Matching condition for the ***port*** or ***length*** argument, according to one of the keywords listed in Table 2.
port	Optional. TCP or UDP source or destination port. This argument is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 3 and Table 4.
range ***port end-port***	Optional. 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. This construct is only available if you specify TCP or UDP as the protocol. The range of values is 1 to 65,535 or one of the keywords listed in Table 3 and Table 4.
dest	Optional. Destination address to be included in the permit or deny criteria. An IP address in the form ***A.B.C.D***.
dest-wildcard	Indication of which bits in the ***dest*** argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. 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.
host ***dest***	Address of a single-host destination with no wildcard address bits. The **host** ***dest*** construct is identical to the ***dest dest-wildcard*** construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
length	Optional. Indicates that packet length is to be used as a filter. The packet length is the length of the network-layer packet, beginning with the IP header, regardless of the specified protocol.
length	Packet length. The range of values is 20 to 65,535.
range ***length end-length***	Packets that fall into the range of specified lengths. Each value (***length*** and ***end-length***) can be from 20 to 65,535.
icmp-type ***icmp-type***	Optional. Type of ICMP packet to be matched. The range of values is 0 to 255 or one of the keywords listed in Table 5. This argument is only available if you specify **icmp** for the ***protocol*** argument.
icmp-code ***icmp-code***	Optional if you use the **icmp-type** ***icmp-type*** construct. A particular ICMP message code to be matched. The range of values is 0 to 255. This argument is only accepted if you specified **icmp** for the ***protocol*** argument.
igmp-type ***igmp-type***	Optional. Type of IGMP packet to be matched. This argument is only accepted if you specified **igmp** as the ***protocol*** argument The range of values is 0 to 15 or one of the keywords listed in Table 5.

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 7.
established	Optional. Specifies that only established connections are to be matched. 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: • SYN • SYN+ACK • ACK • PSH+ACK • URG+ACK • URG+PSH+ACK • FIN • FIN+ACK • RST • RST+ACK 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. 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. 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, with 7 being the highest precedence, or one of the keywords listed in Table 8.
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 9.

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.
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.

1.12.4 Default

None

1.12.5 Usage Guidelines

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

To explicitly set the order of the statement in an ACL, use the **seq deny** 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.

- 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. Be aware that 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 coming in 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.

The following tables list the valid keyword values for the *protocol* argument in statements for IPv4 ACLs, see Table 1.

Table 1 Valid Keyword Values for the protocol Argument for statements in IPv4 ACLs

Keyword	Definition
ahp	Authentication Header Protocol.
esp	Encapsulation Security Payload.
gre	Generic Routing Encapsulation.
host	Host source address.
icmp	Internet Control Message Protocol.
igmp	Internet Group Management Protocol.
ip	Any IP protocol.
ipinip	IP-in-IP tunneling.
ospf	Open Shortest Path First.
pcp	Payload Compression Protocol.
pim	Protocol Independent Multicast.
tcp	Transmission Control Protocol.
udp	User Datagram Protocol.

Table 2 lists the valid keyword values for the ***cond*** argument.

Table 2 Valid Keyword Values for the cond Argument

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

Table 3 lists the valid keyword values for the ***port*** argument when it is used to specify a TCP port.

Table 3 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 3 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

Table 3 Valid Keyword Values for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
whois	Nickname	43
www	World Wide Web (HTTP)	80

Table 4 lists the valid keyword values for the ***port*** argument when it is used to specify a UDP port.

Table 4 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

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

Keyword	Definition	Corresponding Port Number
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 5 lists the valid keyword values for the ***icmp-type*** argument.

Table 5 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

Table 5 Valid Keyword Values for the icmp-type Argument

Keyword	Description
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
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 6 lists the valid keyword values for the ***igmp-type*** argument.

Table 6 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 7 lists the valid keyword values for the ***dscp-value*** argument.

Table 7 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

Table 7 Valid Keyword Values for the dscp-value Argument

Keyword	Definition
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 8 lists the valid keyword values for the ***prec-value*** argument.

Table 8 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 9 lists the valid keyword values for the ***tos-value*** argument.

Table 9 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).

1.12.6 Examples

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

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

1.13 deny (IPv6 ACL)

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

deny [*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*

1.13.1 Purpose

Creates an IPv6 access control list (ACL) statement that denies packets that match the specified criteria.

1.13.2 Command Mode

Access control list configuration

1.13.3 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 Table 10.
src-ipv6-address/prefix-length	The traffic source to add to the statement criteria. The *src-ipv6-address/prefix-length* argument is in the format A:B:C:D::E/*prefix -length*, where the prefix length can be a number from 0 to 128.
any	Indicates that IP traffic to or from all IP addresses is to be included in the **deny** criteria.
cond	Required if you specify the TCP or UDP protocol. Matching condition according to one of the keywords listed in Table 11.
range *port end-port*	Optional if you specify the TCP or UCP protocol. Beginning and ending TCP or UDP source or destination ports that define a range of port numbers. A packet's port must fall 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 12 and Table 13.

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 14. 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. This keyword is available only 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: • SYN • SYN+ACK • ACK • PSH+ACK • URG+ACK • URG+PSH+ACK • FIN • FIN+ACK • RST • RST+ACK 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. This keyword is available only if you specify **tcp** for the ***protocol*** argument. Although you can permit or deny invalid TCP flags, we recommend that you deny them 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 15.
fragments	Optional. Permits or denies a packet based on whether the packet is fragmented. This keyword matches an IPv6 packet, if it has a fragment type extension header. (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 with IPv6 administrative ACLs.

(1) On Layer 4 (L4) parameters such as UDP and TCP ports, only one fragment contains a specific L4 field—in most cases, the first fragment. Although the ACL is applied to all fragments, in most cases no matches occur except for the first fragment.

1.13.4 Default

None

1.13.5 Usage Guidelines

Use the **deny** command to create an IP ACL statement to deny packets that match the specified criteria. This command does not set the order of the statement in the ACL; the OS automatically sets the order. Use the **seq deny** command to set the order of the statement in the ACL.

In IPv6 statements, a total of 100 rules can be added to an ACL, and IPv6 administrative ACLs (in contexts) automatically enable IPv6 Neighbor Discovery.

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 **deny ipv6 any any** or **deny ipv6** *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 10 lists the valid keyword values for the *protocol* argument:

Table 10 Valid Keyword Values for the protocol Argument

icmp	Specifies 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	Specifies 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	Specifies Open Shortest Path First.
pcp	Payload Compression Protocol
pim	Specifies Protocol Independent Multicast.
tcp	Specifies Transmission Control Protocol.
udp	Specifies User Datagram Protocol.

Table 11 lists the valid keyword values for the *cond* argument.

Table 11 Valid Keyword Values for the cond Argument

Keyword	Description
eq	Equal to

Table 11 Valid Keyword Values for the cond Argument

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

Table 12 lists the valid keyword values for the ***`port`*** argument when it is used to specify a TCP port.

Table 12 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

Table 12 Valid Keyword Values for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
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 13 lists the valid keyword values for the ***port*** argument when it is used to specify a UDP port.

Table 13 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

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

Keyword	Definition	Corresponding Port Number
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 14 lists the valid keyword values for the ***icmp-type*** argument.

Table 14 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

Table 14 Valid Keyword Values for the icmp-type Argument

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

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

Table 15 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

1.13.6 Examples

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

1.14 deny (service policy)

deny {**context name** *ctx-name* | **domain name** *name* | **pppoe service-name** *name* | **dhcp hostname** *name*}

no deny {**context name** *ctx-name* | **domain name** *name* | **pppoe service-name** *name* | **dhcp hostname** *name*}

1.14.1 Purpose

Denies access to the specified context, Point-to-Point over Ethernet (PPPoE) service, or domain for PPPoE subscriber sessions that are attached to the service policy. This command also denies a DHCP client host access to the circuit that is associated with the service policy.

1.14.2 Command Mode

Service policy configuration

1.14.3 Syntax Description

context name *ctx-name*	Denies subscriber sessions access to the specified context.
domain name *name*	Denies subscriber sessions access to the specified domain.
pppoe service-name *name*	Denies PPPoE Active Discovery Initiation (PADI) or PPPoE Active discovery Request (PADR) packets access to the specified PPPoE service.
dhcp hostname *name*	Denies the specified DHCP client host access to the circuit that is associated with the service policy.

1.14.4 Default

None

1.14.5 Usage Guidelines

Use the **deny** command to deny access to the specified context, PPPoE service, or domain for subscriber PPPoE sessions that are attached to the service policy. You can also use the **deny** command to deny a DHCP client host access to the circuit that is associated with the service policy.

Any DHCP hosts, contexts, PPPoE services, or domains that are not explicitly specified through this command are implicitly allowed.

Note: The router does not support both allow and deny in the same service profile.

Use the **no** form of this command to allow access to a prohibited context, PPPoE service, or domain. Or, you can use the **no** form of this command to remove a configuration that denies a DHCP client host access to the circuit that is associated with the service policy.

1.14.6 Examples

The following example shows how to configure a service policy, **local-only**, which denies subscriber access to the **ctx_black** context and **dmn_black** domain:

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#deny context name ctx_black
[local]Redback(config-policy-svc)#deny domain name dmn_black
```

The following example shows how to create a service policy called **AllowData**, which denies the PPPoE service named **voice** and allows all other PPPoE services:

```
[local]Redback(config)#service-policy name AllowData

[local]Redback(config-policy-svc)#deny pppoe service-name voice
```

The following example shows how to create a service policy called deny hosts, which denies the DHCP client hosts named `group1`, `group4`, and `group5` access to the circuit that is associated with the specified service policy and allows all other DHCP client hosts to access the circuit:

```
[local]Redback(config)#service-policy name denyhosts

[local]Redback(config-policy-svc)#deny dhcp hostname group1

[local]Redback(config-policy-svc)#deny dhcp hostname group4

[local]Redback(config-policy-svc)#deny dhcp hostname group5
```

1.15 description (ACL)

description *text*

no description

1.15.1 Purpose

Associates a text description with an IP access control list (ACL) or a policy ACL.

1.15.2 Command Mode

Access control list configuration

1.15.3 Syntax Description

text	Alphanumeric text description to be associated with the ACL.

1.15.4 Default

No description is associated with the ACL.

1.15.5 Usage Guidelines

Use the **description** command to associate a text description with the ACL.

You can use a text description to notate what an ACL consists of or how it is to be used. Only one description can be associated with a single ACL. To revise a description, create a new one, and the old one is overwritten.

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

1.15.6 Examples

The following example shows how to create a text description to be associated with the IP ACL, **restricted:**

```
[local]Redback(config-ctx)#ip access-list restricted
[local]Redback(config-access-list)#description private net
```

The following example shows how to create a text description to be associated with the policy ACL, **trafficin:**

```
[local]Redback(config-ctx)#policy access-list trafficin

[local]Redback(config-access-list)#description inbound traffic web
```

1.16 description (APS)

description *text*

{**no** | **default**} **description** [*text*]

1.16.1 Purpose

Associates textual information with an Automatic Protection Switching (APS) or Multiplex Section Protection (MSP) group.

1.16.2 Command Mode

APS configuration

1.16.3 Syntax Description

text	Text string that identifies the port. The string can be any alphanumeric string, including spaces, that is not longer than 63 ASCII characters.

1.16.4 Default

No description is associated with an APS/MSP group.

1.16.5 Usage Guidelines

Use the **description** command to associate textual information with an APS/MSP group. The **show configuration** command displays this text for the APS/MSP group.

Use the **no** or **default** form of this command to delete the existing description. Because only one description for an APS/MSP group can exist, when you use the no or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.16.6 Examples

The following example shows how to associate a description with the APS/MSP group **lab48:**

```
[local]Redback(config)#aps group lab48 pos
[local]Redback(config-aps)#description OC-48 APS
```

1.17 description (ATM, Frame Relay)

description *text*

{**no** | **default**} **description**

1.17.1 Purpose

Associates a textual description with an Asynchronous Transfer Mode (ATM) or Frame Relay profile or permanent virtual circuit (PVC).

1.17.2 Command Mode

- ATM profile configuration
- ATM PVC configuration
- Frame Relay profile configuration
- Frame Relay PVC configuration

1.17.3 Syntax Description

text	Text string that identifies the profile or PVC. Can be any alphanumeric string, including spaces, not to exceed the following lengths: • 79 ASCII characters in Frame Relay profile and Frame Relay PVC configuration mode • 255 characters in ATM profile and ATM PVC configuration mode

1.17.4 Default

No description is associated with any profile or PVC.

1.17.5 Usage Guidelines

Use the **description** command to associate textual information with an ATM or Frame Relay profile or PVC. This text is displayed by the appropriate **show** command.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a profile or PVC, when you use the **no** or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.17.6 Examples

The following example shows how to associate a description with an ATM PVC configured on an ATM OC port:

```
[local]Redback(config)#port atm 2/1

[local]Redback(config-atm-oc)#atm pvc 0 32 profile dslam1 encapsulation bridge1483

[local]Redback(config-atm-pvc)#description ATM bridged 1483 circuit
```

1.18 description (BGP)

description ***text***

no description

1.18.1 Purpose

Associates a description with the Border Gateway Protocol (BGP) neighbor or peer group.

1.18.2 Command Mode

- BGP neighbor configuration
- BGP peer group configuration

1.18.3 Syntax Description

text	Description of the neighbor (maximum of 80 characters).

1.18.4 Default

None

1.18.5 Usage Guidelines

Use the **description** command to associate a description with the BGP neighbor or peer group. This command does not affect the BGP connection. It is used as a note in the configuration.

Use the **no** form of this command to remove a description from the configuration. Because there can be only one description for a BGP neighbor or peer group, when you use the **no** form of this command, it is not necessary to include the ***text*** argument.

1.18.6 Examples

The following example shows how to provide the description, **Palo Alto BGP Neighbor 12**, for the BGP neighbor at IP address, **102.210.210.1:**

```
[local]Redback(config-ctx)#router bgp 100
[local]Redback(config-bgp)#neighbor 102.210.210.1 external
[local]Redback(config-bgp-neighbor)#description Palo Alto BGP Neighbor 12
```

1.19 description (bridge)

description *text*

{**no** | **default**} **description**

1.19.1 Purpose

Associates a textual description with a bridge.

1.19.2 Command Mode

Bridge configuration

1.19.3 Syntax Description

text	Text string that identifies the bridge. Can be any alphanumeric string, including spaces, that is not longer than 63 ASCII characters.

1.19.4 Default

No description is associated with any bridge.

1.19.5 Usage Guidelines

Use the **description** command to associate textual information with a bridge. This text displays by the appropriate **show** command.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a bridge, when you use the **no** or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.19.6 Examples

The following example shows how to associate a description with the bridge, **isp1**, configured in the **bridge** context:

```
[local]Redback(config)#context bridge
[local]Redback(config-ctx)#bridge isp1
[local]Redback(config-bridge)#description Bridge for all traffic to ISP1
```

1.20 description (Dot1Q)

description *text*

{**no** | **default**} **description**

1.20.1 Purpose

Associates a textual description with an 802.1Q profile or permanent virtual circuit (PVC).

1.20.2 Command Mode

- dot1q profile configuration
- dot1q PVC configuration

1.20.3 Syntax Description

text	Text string that identifies the profile or PVC. Can be any alphanumeric string, including spaces, not to exceed the following lengths: • 100 ASCII characters in dot1q profile configuration mode • 255 characters in dot1q PVC configuration mode

1.20.4 Default

No description is associated with any profile or PVC.

1.20.5 Usage Guidelines

Use the **description** command to associate textual information with an 802.1Q profile or PVC. This text is displayed by the appropriate **show** command.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a profile or PVC, when you use the **no** or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.20.6 Examples

The following example provides the description, **local vlan**, for the 802.1Q PVC `100`:

```
[local]Redback(config-port)#dot1q pvc 100
[local]Redback(config-dot1q-pvc)#description local vlan
```

1.21 description (interface)

description ***text***

{**no** | **default**} **description**

1.21.1 Purpose

Associates a text description with an interface.

1.21.2 Command Mode

Interface configuration

1.21.3 Syntax Description

text	Text string, up to 255 ASCII characters, that identifies the interface.

1.21.4 Default

None

1.21.5 Usage Guidelines

Use the **description** command to associate a text description with an interface. The description appears in the output of the **show ip interface** and **show configuration** commands. Text can be any alphanumeric string, including spaces. For more information on the **show configuration** command, see *Using the CLI*.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for an interface, you can omit the ***text*** argument when you use the **no** form of this command. To change a description, create a new one; it overwrites the existing one.

1.21.6 Examples

The following example shows how to create the interface, **upstream**, as the upstream interface to the **goldisp.net** service provider:

```
[local]Redback(config-ctx)#interface upstream
[local]Redback(config-if)#description interface to goldisp.net
```

1.22 description (L2TP peer)

description ***text***

{**no** | **default**} **description**

1.22.1 Purpose

Associates textual information with a Layer 2 Tunneling Protocol (L2TP) peer.

1.22.2 Command Mode

L2TP peer configuration

1.22.3 Syntax Description

text	Textual description for an L2TP peer. Can be any alphanumeric string, including spaces, up to 255 ASCII characters.

1.22.4 Default

No description is associated with the L2TP peer.

1.22.5 Usage Guidelines

Use the **description** command to associate textual information with the L2TP peer. The description appears in the output of the **show configuration** command with the **l2tp** keyword in any mode.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a peer, when you use the no form of this command, it is not necessary to include the text argument.

To change a description, create a new one; it overwrites the existing one.

1.22.6 Examples

The following example shows how to select (or create) an L2TP peer, and then associates a text description with it:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#l2tp-peer name isp1.net remote 172.16.1.2 local 172.16.1.1
[local]Redback(config-l2tp)#description Corporate offices in Connecticut
```

The following example shows how to change the description created in the previous example:

```
[local]Redback(config-l2tp)#description Corporate offices in Hartford
```

The following example shows how to delete an existing description:

```
[local]Redback(config-l2tp)#no description
```

1.23 description (link group)

description ***description***

no description

1.23.1 Purpose

Specifies a text string description of the access link group.

1.23.2 Command Mode

Link group configuration

1.23.3 Syntax Description

description

Text string description of the link group.

For access link groups only, this string is used as the prefix to the NAS-PORT-ID RADIUS attribute (prefix-nas-port-id) if and only if the **radius attribute nas-port-id** command using the **format modified-agent-circuit-id prefix-lg-description** keywords has been entered. If no description is provided by this command, the default prefix is `eth`.

1.23.4 Default

The link group has no description in the default state.

1.23.5 Usage Guidelines

Use the **description** command in link group configuration mode to specify a text string description of the access link group.

For access link groups, the description can be used as a prefix to the RADIUS NAS-PORT-ID attribute. Enter a unique ID for each access link group.

Use the **no** form of this command to delete the description.

1.23.6 Examples

The following example illustrates the use of the **description** command:

```
[local]Redback(config)#link-group lg1 access
[local]Redback(config-link-group)#description 35ttf
```

1.24 description (lists)

description *text*

no description

1.24.1 Purpose

Associates a description with the autonomous system (AS) path list, community list, extended community list, IP prefix list, or IP Version 6 (IPv6) prefix list.

1.24.2 Command Mode

- AS path list configuration
- Community list configuration
- Extended community list configuration
- IP prefix list configuration
- IPv6 prefix list configuration

1.24.3 Syntax Description

text	Description of the AS path list, community list, extended community list, IP prefix list, or IPv6 prefix list.

1.24.4 Default

None

1.24.5 Usage Guidelines

Use the **description** command to associate a description with the AS path list, community list, extended community list, IP prefix list, or IPv6 prefix list. For more information, see the **as-path-list**, **community-list**, **ext-community-list**, **ip prefix-list**, and **ipv6 prefix-list** commands in context configuration mode.

Use the **no** form of this command to remove a description. Because there can be only one description for an AS path list, community list, extended community list, IP prefix list, or IPv6 prefix list, when you use the **no** form of this command, it is not necessary to include the *text* argument.

1.24.6 Examples

The following example shows how to configure a description for the community list, **com-list1:**

```
[local]Redback(config-ctx)#community-list com-list1
[local]Redback(config-community-list)#description filter for community1
```

1.25 description (MPLS static and RSVP LSPs)

description ***text***

no description

1.25.1 Purpose

Associates a description with a static label-switched path (LSP) or a Resource Reservation Protocol (RSVP) LSP.

1.25.2 Command Mode

- MPLS static LSP configuration
- RSVP LSP configuration

1.25.3 Syntax Description

text	Description of the LSP (maximum of 80 characters).

1.25.4 Default

None

1.25.5 Usage Guidelines

Use the **description** command to associate a description with a static LSP or an RSVP LSP. This command does not affect the LSP; it is used only as a note in the configuration.

Use the **no** form of this command to remove a description from the configuration. Because there can be only one description for an LSP, when you use the **no** form of this command, it is not necessary to include the ***text*** argument.

1.25.6 Examples

The following example shows how to provide the description, **Shortcut to Net 41A**, for the MPLS static LSP, **To41A:**

```
[local]Redback(config)#context sj1
[local]Redback(config-ctx)#router mpls-static
[local]Redback(config-mpls-static)#lsp To41A
[local]Redback(config-mpls-static-lsp)#description Shortcut to Net 41A
[local]Redback(config-mpls-static-lsp)#
```

1.26 description (MSDP peers)

description ***text***

no description

1.26.1 Purpose

Associates a text description with a Multicast Source Discovery Protocol (MSDP) peer.

1.26.2 Command Mode

MSDP peer configuration

1.26.3 Syntax Description

text	Text string that identifies the MSDP peer.

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **description** command to associate a text description with an MSDP peer. The description can be a maximum of 80 characters.

Use the **no** form of this command to remove the description from the MSDP peer. Because there can be only one description for an MSDP peer, when you use the **no** form of this command, it is not necessary to include the ***text*** argument.

1.26.6 Examples

The following example shows how to set the MSDP peer description to **Peer66 to used for testing:**

```
[local]Redback(config-msdp)#peer 192.168.1.1 local-tcp-source peer66
[local]Redback(config-msdp-peer)#description Peer66 to used for testing
```

1.27 description (port)

description *text*

{**no** | **default**} **description**

1.27.1 Purpose

Associates textual information with a port.

1.27.2 Command Mode

- ATM OC configuration
- Interface configuration
- Port configuration

1.27.3 Syntax Description

text	Text string that identifies the port. Can be any alphanumeric string, including spaces. The string may not exceed 255 ASCII characters.

1.27.4 Default

No description is associated with a port.

1.27.5 Usage Guidelines

Use the **description** command to associate textual information with the port. The show port detail command for the port displays this text.

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a port, when you use the **no** or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.27.6 Examples

The following example shows how to associate a description with the management port on the controller card in slot **7:**

```
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#description Management port
```

1.28 description (port, channel)

description *text*

{**no** | **default**} **description**

1.28.1 Purpose

Associates a text description with a port or channel.

1.28.2 Command Mode

- ATM OC configuration
- Interface configuration
- Port configuration
- STM-1 configuration

1.28.3 Syntax Description

text	Text string that identifies the channel. Can be any alphanumeric string, including spaces, that is not longer than 255 ASCII characters.

1.28.4 Default

No description is associated with a port or channel.

1.28.5 Usage Guidelines

Use the **description** command to associate a text description with a port or channel. This text appears in the output of the **show port detail** command (in any mode).

Use the **no** or **default** form of this command to delete the existing description. Because there can be only one description for a port or channel; when you use the **no** or **default** form of this command, it is not necessary to include the text argument. To change a description, create a new one; it overwrites the existing one.

1.28.6 Examples

The following example shows how to associate a description with channelized OC-12 port **1** in slot **4:**

```
[local]Redback(config)#port channelized-oc12 4/1

[local]Redback(config-port)#description channelized OC-12 in New York
```

1.29 description (snmp alarm)

description ***description***

no description

1.29.1 Purpose

Describes the alarm model.

1.29.2 Command Mode

SNMP alarm model configuration

1.29.3 Syntax Description

description	A word or phrase that describes the alarm model.

1.29.4 Default

None

1.29.5 Usage Guidelines

Use the **description** command to describe the alarm model you are configuring.

Use the **no** form to remove the description of the alarm model.

1.29.6 Examples

The following example shows how to configure the description of an alarm model to **LinkUp Administrative**.

```
[local]jazz#config
[local]jazz(config)#snmp alarm model 1 state major
[local]jazz(config-snmp-alarmmodel)#description LinkUp Administrative
[local]jazz(config-snmp-alarmmodel)#exit
```

1.30 description (SSE)

description *text*

{**no** | **default**} **description** *text*

1.30.1 Command Mode

SSE group configuration

1.30.2 Syntax Description

text	Text description associated with the SSE group.

1.30.3 Default

No description is associated with the SSE group.

1.30.4 Usage Guidelines

Associates a text description with an SSE group. Only one description can be associated with an SSE group. To revise a description, create a new one, and the old one is overwritten.

Use the **no** or **default** form of this command to delete the existing description.

1.30.5 Examples

```
[local]Redback(config)#sse group sse_group_1 network-redundant
[local]Redback(config-SE-group)#description SSE group 1
```

1.31 description (tunnel)

description ***text***

no description

1.31.1 Purpose

Associates textual information with the tunnel.

1.31.2 Command Mode

Tunnel configuration

1.31.3 Syntax Description

text	Textual description for a tunnel. Can be any alphanumeric string, including spaces, not to exceed 64 ASCII characters.

1.31.4 Default

No description is associated with the tunnel.

1.31.5 Usage Guidelines

Use the **description** command to associate textual information with the tunnel. The description appears in the output of the **show configuration** command with the **tunnel** keyword (in any mode).

Use the **no** form of this command to delete the existing description. Because there can be only one description for a tunnel, when you use the no form of this command, it is not necessary to include the text argument.

To change a description, create a new one; it overwrites the existing one.

1.31.6 Examples

The following example shows how to select (or create) a GRE tunnel, and then associate a text description with it:

```
[local]Redback(config)#tunnel gre HartfordTnl
[local]Redback(config-tunnel)#description Corporate offices in Hartford
```

The following example shows how to change the description created in the previous example:

```
[local]Redback(config-tunnel)#description Branch offices in Hartford
```

The following example shows how to delete an existing description:

```
[local]Redback(config-tunnel)#no description
```

1.32 description (VPLS profiles)

description *text*

no description

1.32.1 Purpose

Associates a description with a neighbor.

1.32.2 Command Mode

VPLS profile neighbor configuration

1.32.3 Syntax Description

text	Description of the neighbor (63 characters maximum).

1.32.4 Default

None

1.32.5 Usage Guidelines

Use the **description** command to associate a description with a neighbor. This command does not affect the neighbor, but is used only as a note in the configuration.

Note: The neighbor is identified by the IP address of the remote provider edge (PE) device.

Use the **no** form of this command to remove a description from the neighbor. Because there can be only one description for a neighbor, when you use the **no** form of this command, it is not necessary to include the *text* argument.

1.32.6 Examples

The following example shows how to provide the description, **test-peer**, for the neighbor, **10.10.10.1:**

```
[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)#description test-peer
[local]Redback(config-vpls-profile-neighbor)#
```

1.33 destination

destination ***ip-addr*** [***context-name***]

1.33.1 Purpose

Configures the Network Address Translation (NAT) policy or its class to use the specified IP address in destination IP address translation or destination NAT (DNAT).

1.33.2 Command Mode

- NAT policy configuration
- NAT policy class configuration

1.33.3 Syntax Description

ip-addr	Specifies the IP address to replace the original destination address.
context-name	Specifies the name of the context in which the configured destination IP address resides.

1.33.4 Default

No predefined IP address is configured as a destination IP address.

1.33.5 Usage Guidelines

Use the **destination** command to configure the NAT policy or its class to use the specified IP address in DNAT. DNAT replaces the original destination IP addresses of all packets or the packets of a specific class with a predefined IP address.

When a destination IP address is configured for a given class, the SmartEdge router applies this predefined IP address to all packets of the class.

You can enable DNAT with or without having to perform NAT.

Note: If you configure DNAT with NAT, the context name specified in the **destination** command must be the same as the context name specified in the **pool** command.

Configuring DNAT without NAT requires that you configure the **destination** command with the **ignore** command.

Use the **destination***ip-addrr context-name* construct to specify that the configured destination IP address resides within the specified context. Without the name of the context specified, the configured destination IP address is assumed to be either in the context in which the NAT pool is defined or, if no NAT pool is defined, in the context in which the NAT policy is defined.

1.33.6 Examples

The following example shows how to configure DNAT with NAT. A predefined destination address is configured for the NAT-CLASS1 class within the NAT policy NAT-POLICY. For all packets from class NAT-CLASS1, the destination address of each packet is replaced by 64.233.267.100 so that all packets from class NAT-CLASS1 are forwarded to that address. On the return path, a reverse translation from 64.233.267.100 to the original destination address is performed so that the returning traffic appears to be sent from the original destination address:

```
[local]Redback(config-ctx)#nat policy NAT-POLICY
!Default class
[local]Redback(config-policy-nat)#pool NAT-POOL-DEFAULT local
!Named classes
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class NAT-CLASS1
[local]Redback(config-policy-acl-class)#pool NAT-POOL1 local
[local]Redback(config-policy-acl-class)#destination 64.233.167.100
```

The following example shows how to configure DNAT without NAT. A predefined destination address is configured for the NAT-CLASS2 class within the NAT policy NAT-POLICY. For the NAT-CLASS2 class within the NAT policy NAT-POLICY, the destination address of each packet is replaced by 64.233.267.100 so that all packets from class NAT-CLASS2 are forwarded to that address. In this example, the source address is not translated:

```
[local]Redback(config-ctx)#nat policy NAT-POLICY
!Default class
[local]Redback(config-policy-nat)#pool NAT-POOL-DEFAULT local
!Named classes
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class NAT-CLASS2
[local]Redback(config-policy-acl-class)#ignore
[local]Redback(config-policy-acl-class)#destination 64.233.167.100
```

1.34 destination (NAT logging profile)

destination ***ip-addr*** **[context** ***context_name*****] port** ***port-number***

no destination ***ip-addr*** **[context** ***context_name*****] port** ***port-number***

1.34.1 Purpose

Configures a NAT logging profile that sends log messages to the specified destination IP addresses and ports in a given context, by using the source IP address and the source port in the UDP packet.

1.34.2 Command Mode

1.34.3 Syntax

ip-addr	Specifies the IP address of the NetFlow collector where the packet is sent to.
context-name	Specifies the destination context. If the context is not specified, the system defaults to the context where the logging profile is define.
port-number	Specifies the L4 port.

1.34.4 Default

None.

1.34.5 Usage Guidelines

Use the **destination** command to configure a NAT logging profile. This command specifies the following:

- Destination context name of the NetFlow Collector
- Destination IP addresses of the NetFlow Collector
- Destination ports of the NetFlow Collector

The **destination** command is a mandatory field with an optional context configuration where ***ip-addr*** is the IP address of the NetFlow Collector where the packet will be sent to. ***context_name*** defines the destination context. If no context is specified, the system defaults to the context where the logging profile is defined. ***port-number*** is the L4 port.

For more information about how to configure NAT logging, see *nat logging-profile* and *Configure an Enhanced NAT Policy with Logging and Paired Mode*.

1.34.6 Example

This example shows you how to configure a NAT logging profile that sends log messages to the specified destination IP addresses and ports in a given context (local context) , by using source IP address, `100.1.1.1`, and the source port, `8989`, in the UDP packet. n

```
[local]Redback#configuration
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat ?
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
[local]Redback(config-ctx)#nat logging-profile nat-log-profile
[local]Redback(config-nat-profile)#destination 100.1.1.1 context local port 8989
```

1.35 detection-multiplier

detection-multiplier ***value***

{**no** | **default**} **detection-multiplier**

1.35.1 Purpose

Specifies the detection multiplier value.

1.35.2 Command Mode

- BFD interface configuration
- BFD neighbor configuration

1.35.3 Syntax Description

value	Detection multiplier value. The range of values is 1 to 10; the default value is 3.

1.35.4 Default

The default detection multiplier value is 3.

1.35.5 Usage Guidelines

Use the **detection-multiplier** command to specify the detection multiplier value.

The negotiated minimum transmit interval (the minimum desired transmit interval agreed upon by both peers) is multiplied by the detection multiplier value to provide the detection time for the transmitting system in asynchronous mode. The detection time is the time it takes to declare a neighbor as down. For example, if the minimum desired transmit interval was negotiated at 10 ms and the detection multiplier is set to 3, then the detection time is 30 ms. Using the detection multiplier adds robustness to Bidirectional Forwarding Detection (BFD) by allowing the system to not bring down a neighbor if only one BFD packet is missed.

Use the **no** or **default** form of this command to return the detection multiplier value to 3.

1.35.6 Examples

The following example shows how to set the detection multiplier value on the interface, **to_foo**, to **7:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router bfd
[local]Redback(config-bfd)#interface to_foo
[local]Redback(config-bfd-if)#detection-multiplier 7
[local]Redback(config-bfd-if)#
```

1.36 dhcp max-addrs

dhcp max-addrs ***max-sub-addrs***

no dhcp max-addrs

1.36.1 Purpose

Indicates that associated hosts are to use Dynamic Host Configuration Protocol (DHCP) to dynamically acquire address information for the subscriber's circuit, and sets a maximum number of IP addresses that the SmartEdge router expects the external DHCP server to assign to hosts associated with the circuit.

1.36.2 Command Mode

Subscriber configuration

1.36.3 Syntax Description

max-sub-addrs	Maximum number of unique IP addresses the SmartEdge router expects the external DHCP server to assign to hosts associated with a given subscriber circuit. The range of values is 1 to 100. For dynamic clientless IP service selection (CLIPS) subscribers, the value for the ***max-sub-addrs*** argument must be 1.

1.36.4 Default

None

1.36.5 Usage Guidelines

Use the **dhcp max-addrs** command to indicate that associated hosts are to use DHCP to dynamically acquire address information for the subscriber's circuit, and to set a maximum number of IP addresses that the SmartEdge router expects the external DHCP server to assign to hosts associated with the circuit.

For non-CLIPS subscribers, the SmartEdge router deducts the value of the ***max-sub-addrs*** argument from the value for the ***max-dhcp-addrs*** argument that you configured for a DHCP proxy or DHCP relay interface, using the **dhcp proxy** or **dhcp relay** commands (in interface configuration mode), available at the time a subscriber is bound to a circuit. When the value for the

max-dhcp-addrs argument for a DHCP proxy or DHCP relay interface reaches 0, that interface is no longer available for subscriber bindings.

For dynamic CLIPS subscribers, configure the subscriber record or profile with no IP address and specify 1 as the value for the ***max-sub-addrs*** argument; for information about CLIPS, see *Configuring CLIPS*.

Use the **no** form of this command to disable the use of DHCP for the subscriber's circuit.

Note: If you configure a subscriber record with a **dhcp max-addrs** command and with one or more static IP host addresses, using the **ip address** command (in interface configuration mode), the static IP addresses always take precedence; the associated circuit is bound to an interface on the basis of the static IP addresses. If you configure the record with a **dhcp max-addrs** command, and you do not configure any static addresses for it, the associated circuit is bound to the first available interface with capacity for this subscriber.

1.36.6 Examples

The following example shows how to configure the subscriber, **dhcp-test**, to expect a total of **8** IP addresses that can be assigned at any time:

```
[local]Redback(config-ctx)#subscriber name dhcp-test
[local]Redback(config-sub)#dhcp max-addrs 8
```

1.37 dhcp proxy

dhcp proxy ***max-dhcp-addrs*** [**server-group** ***name***]

no dhcp proxy

1.37.1 Purpose

Enables this interface to act as proxy between subscribers and an external Dynamic Host Configuration Protocol (DHCP) server, and access DHCP giaddr configuration mode.

1.37.2 Command Mode

Interface configuration

1.37.3 Syntax Description

max-dhcp-addrs	Maximum number of IP addresses available on the interface. The range of values is 1 to 65,535.
server-group ***name***	Optional. DHCP server group. Forwards all DHCP requests received on the interface to all DHCP servers in the specified server group.

1.37.4 Default

DHCP proxy is disabled.

1.37.5 Usage Guidelines

Use the **dhcp proxy** command to enable this interface to act as a proxy between subscribers and an external Dynamic Host Configuration Protocol (DHCP) server, and access DHCP giaddr configuration mode.

When you enable DHCP proxy, the interface relays all DHCP packets, including the release and renewal of IP addresses for subscriber sessions, between the DHCP server and the subscriber. To the subscriber, the SmartEdge router appears to be the DHCP server.

The SmartEdge router uses the value for the ***max-dhcp-addrs*** argument to load balance between IP addresses from multiple pools. When you configure the SmartEdge router for subscriber DHCP proxy, the value of the ***max-dhcp-addrs*** argument indicates the total number of subscriber requests that will be forwarded on the interface.

The SmartEdge router deducts the ***max-sub-addrs*** value for the **dhcp max-addrs** command (in subscriber configuration mode) from the current value for ***max-dhcp-addrs*** argument for the DHCP proxy interface at the time a subscriber is bound to a circuit using that interface. When the value of ***max-dhcp-addrs*** for a DHCP proxy interface reaches 0, that interface is no longer available for subscriber bindings.

Use the **no** form of this command to disable DHCP proxy on the interface.

Note: You can configure an interface to act as either a DHCP relay or a DHCP proxy; the **dhcp relay** and **dhcp proxy** commands are mutually exclusive.

Note: For the **dhcp proxy** command to take effect, you must configure an external DCHP server, using the **dhcp relay server** command in the context in which the interface is configured.

1.37.6 Examples

The following example shows how to enable the **proxy1** interface to act as a DHCP proxy for the DHCP server at IP address, **10.30.40.50:**

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#interface proxy1
[local]Redback(config-if)#ip address 10.1.2.3 255.255.255.0
[local]Redback(config-if)#dhcp proxy 253
```

1.38 dhcp relay

dhcp relay ***max-dhcp-addrs*** [**server-group** ***group-name***]

no dhcp relay

1.38.1 Purpose

Enables this interface to relay Dynamic Host Configuration Protocol (DHCP) messages to an external DHCP server, and access DHCP giaddr configuration mode.

1.38.2 Command Mode

Interface configuration

1.38.3 Syntax Description

max-dhcp-addrs	Maximum number of IP addresses available on the interface. The range of values is 0 to 65,535.
server-group ***group-name***	Optional. DHCP server group. Forwards all DHCP requests received on the interface to all DHCP servers in the specified server group.

1.38.4 Default

DHCP relay is disabled.

1.38.5 Usage Guidelines

Use the **dhcp relay** command to enable this interface to relay DHCP messages to an external DHCP server, and access DHCP giaddr configuration mode.

The SmartEdge router uses the value for the ***max-dhcp-addrs*** argument to load balance between IP addresses from multiple pools. When you configure the SmartEdge router for subscriber DHCP relay, the value of the ***max-dhcp-addrs*** argument indicates the total number of subscriber requests that can be forwarded on the interface.

The value of the ***max-sub-addrs*** argument for the **dhcp max-addrs** command (in subscriber configuration mode) is deducted from the ***max-dhcp-addrs*** value configured for a DHCP relay interface available at the time a subscriber is bound to a circuit on that interface. When the value of ***max-dhcp-addrs*** for a DHCP relay interface reaches 0, that interface is no longer available for subscriber bindings.

Note: You can configure an interface to act as either a DHCP relay or a DHCP proxy; the **dhcp relay** and **dhcp proxy** commands are mutually exclusive.

Note: For the **dhcp relay** command to take effect, you must configure an external DCHP server, using the **dhcp relay server** command in the context in which the interface is configured.

Use the **no** form of this command to disable DHCP relay on the interface.

1.38.6 Examples

The following example shows how to enable DHCP relay on interface **eth1**, which is configured with a total of **253** IP addresses that can be allocated by the DHCP server at any time from the **10.1.1.0** subnet:

```
[local]Redback(config-ctx)#interface eth1
[local]Redback(config-if)#ip address 10.1.1.0 255.255.255.0
[local]Redback(config-if)#dhcp relay 253
[local]Redback(config-dhcp-giaddr)#
```

1.39 dhcp relay option

dhcp relay option [**hostname** [**separator** *character*]]

no dhcp relay option [**hostname** [**separator** *character*]]

1.39.1 Purpose

Enables sending Dynamic Host Configuration Protocol (DHCP) options in DHCP packets relayed by the interfaces in the specified context.

1.39.2 Command Mode

Context configuration

1.39.3 Syntax Description

hostname	Optional. Prepends the SmartEdge router hostname to the agent circuit id field of DHCP option 82. The SmartEdge router uses the hostname that you have configured using the **system hostname** command (in context configuration mode). If you have not configured the hostname, the SmartEdge router uses the default hostname of “Redback.”
separator *character*	Optional. Character that separates the elements of the attribute string. Changes the character that separates the hostname from the circuit id field of DCHP option 82. The default separator character is the colon (**:**).

1.39.4 Default

DHCP options are not sent.

1.39.5 Usage Guidelines

Use the **dhcp relay option** command to enable sending DHCP options in all DHCP packets that are relayed by the interfaces in the specified context.

On some networks, DHCP is used to dynamically configure IP address information for subscriber hosts.

The SmartEdge router can act as a relay or as a proxy for DHCP servers. DHCP is typically used with RFC 1483 bridge-encapsulated circuits, and not Point-to-Point Protocol (PPP) circuits.

The SmartEdge router can use DHCP relay options to help track DHCP requests. Some options can also enhance the DHCP server’s function.

The DHCP relay options are described in RFC 3046, `DHCP Relay Agent Information Option`.

For relay options to take effect, enable DHCP relay for the context, using the **`dhcp relay server`** command (in context configuration mode), and for an interface, using the **`dhcp relay`** or **`dhcp proxy`** command (in interface configuration mode).

You must also configure subscriber records, using the **`dhcp max-addrs`** command (in subscriber configuration mode) to indicate that associated hosts are to use DHCP relay to dynamically acquire address information.

Use the **`no`** form of this command to disable the sending of DHCP options.

1.39.6 Examples

The following example shows how to enable sending of DHCP relay options:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option
```

The following example shows how to prepend the system hostname, **TP23**, to the agent circuit id field of DHCP option 82 and, by default, uses the colon (:) to separate the hostname from the circuit id field:

```
[local]Redback(config)#server hostname TP23
[local]Redback(config)#context local
[local]Redback(config-ctx)#dhcp relay server 108.1.1.157
[local]Redback(config-dhcp-relay)#exit
[local]Redback(config-ctx)#dhcp relay option hostname
```

The DHCP server's lease log for this configuration would be similar to the following example:

```
lease 120.1.3.191 {
  starts 2 2005/11/08 10:05:21;
  ends 2 2005/11/08 10:35:21;
  binding state active
  netx binding state free
  hardware ethernet 00:dd:00:00:00:1e;
  uid "\001\006\000\335\000\000\000\036";
option agent.circuit-id "SE800:1/4 vpi-vci 0 103";
}
```

1.40 dhcp relay server

dhcp relay server {*ip-addr* | *hostname*} [**max-hops** *count*] [**min-wait** *interval*]

no dhcp relay server {*ip-addr* | *hostname*} [**max-hops** *count*] [**min-wait** *interval*]

1.40.1 Purpose

Configures an external Dynamic Host Configuration Protocol (DHCP) server and enters DHCP relay server configuration mode.

1.40.2 Command Mode

Context configuration

1.40.3 Syntax Description

ip-addr	IP address of the DHCP server.
hostname	Hostname of the DHCP server.
max-hops *count*	Optional. Maximum number of hops allowed for requests. The range of values for the *count* argument is 1 to 16.
min-wait *interval*	Optional. Minimum time, in seconds, to wait before forwarding requests to the DHCP server. The range of values for the *interval* argument is 0 to 60.

1.40.4 Default

Disabled

1.40.5 Usage Guidelines

Use the **dhcp relay server** command to configure an external DHCP server and enter DHCP relay server configuration mode. You can configure up to five external DHCP servers in each context.

If you have configured RADIUS authentication, the SmartEdge router sends an accounting record to RADIUS every time DCHP assigns or releases an IP address.

Note: For the **dhcp relay server** command to take effect, you must also enable DHCP relay or DHCP proxy on an interface in the same context, using the **dhcp proxy** or **dhcp relay** command (in interface configuration mode).

To indicate that associated hosts are to use DHCP relay to dynamically acquire address information, configure the subscriber default profile, a named profile, or subscriber records with the **dhcp max-addrs** command (in subscriber configuration mode).

Use the **no** form of this command to disable the DHCP server.

1.40.6 Examples

The following example shows how to configure an external DHCP server at IP address, **10.30.40.50**, and enter DHCP relay server configuration mode:

```
[local]Redback(config-ctx)#dhcp relay server 10.30.40.50
[local]Redback(config-dhcp-relay)#
```

1.41 dhcp relay server retries

dhcp relay server retries *count* **timeout** *interval*

no dhcp relay server retries *count* **timeout** *interval*

1.41.1 Purpose

Specifies the number of attempts and the interval to wait for each attempt when trying to reach an external Dynamic Host Configuration Protocol (DHCP) server before it is marked unreachable.

1.41.2 Command Mode

Context configuration

1.41.3 Syntax Description

count	Maximum consecutive number of times to attempt reaching the DHCP server; the default value is 3.
timeout *interval*	Interval, in seconds, to wait for a reply after a DHCP request packet is sent. The default value for the *interval* argument is 30.

1.41.4 Default

Up to three attempts are made to reach a DHCP server, with a wait interval of 30 seconds for each attempt.

1.41.5 Usage Guidelines

Use the **dhcp relay server retries** command to specify the number of attempts and the interval to wait for each attempt when trying to reach an external DHCP server before it is marked unreachable.

If the interval expires without receiving a reply from the DHCP server, another DHCP request is sent to the DHCP server until the maximum consecutive number of attempts has been reached. If the interval expires after the last attempt without reaching the DHCP server, then the DHCP server is marked unreachable.

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

1.41.6 Examples

The following example shows how to configure the SmartEdge router to make up to **5** attempts to reach a DHCP server, with a wait interval of **15** seconds for each attempt:

```
[local]Redback(config-ctx)#dhcp relay server retries 5 timeout 15
[local]Redback(config-ctx)#
```

1.42 dhcp relay suppress-nak

dhcp relay suppress-nak

no dhcp relay suppress-nak

1.42.1 Purpose

Disables sending a DHCPNAK message when the SmartEdge router receives a DHCPREQUEST message for which it does not have an entry.

1.42.2 Command Mode

Context configuration

1.42.3 Syntax Description

This command has no keywords or arguments.

1.42.4 Default

A DHCPNAK message is always sent.

1.42.5 Usage Guidelines

Use the **dhcp relay suppress-nak** command to disable the sending of a DHCPNAK message when the SmartEdge router receives a DHCPREQUEST message for which it does not have an entry. In this case, the request is dropped.

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

1.42.6 Examples

The following example shows how to disable sending a DHCPNAK message:

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

1.43 dhcp server

dhcp server {**interface** | ***ip-addr***}

no dhcp server

1.43.1 Purpose

Enables this interface for internal Dynamic Host Configuration Protocol (DHCP) server support and assigns the IP address to be used for this support.

1.43.2 Command Mode

Interface configuration

1.43.3 Syntax Description

interface	Assigns the primary IP address of the interface to the DHCP server.
ip-addr	One of the secondary IP addresses assigned to the interface.

1.43.4 Default

No internal DHCP servers are created.

1.43.5 Usage Guidelines

Use the **dhcp server** command to enable this interface for internal DHCP server support and assign the IP address to be used for this support.

For information about the **context** command (in global configuration mode), the **interface** command (in context configuration mode), and the **ip address** command (in interface configuration mode), see *Configuring Contexts and Interfaces*.

Note: The actual choice of an IP address for the internal DHCP server is made by authentication, authorization, and accounting (AAA), subject to any static mappings, subnets, and ranges that you have configured for the server.

Note: IP pools on an interface can be used to provide addresses for the DHCP server. If there is no range of values specified on a DHCP subnet, the DHCP server takes the IP addresses from the IP pool defined in the interface command. This IP pool can also be used by the DHCP server and PPP subscribers on the same interface.

Use the **no** form of this command to delete the internal DHCP server.

1.43.6 Examples

The following example shows how to create an internal DHCP server using the secondary IP address for the **dhcp-if** interface in the **dhcp** context:

```
[local]Redback(config)#context dhcp
[local]Redback(config-ctx)#interface dhcp-if multibind
[local]Redback(config-if)#ip address 12.1.1.1/24
[local]Redback(config-if)#ip address 13.1.1.1/24 secondary
[local]Redback(config-if)#dhcp server 13.1.1.1
```

1.44 dhcp server policy

dhcp server policy

no dhcp server policy

1.44.1 Purpose

Enables internal Dynamic Host Configuration Protocol (DHCP) server functions in this context and accesses DHCP server configuration mode.

1.44.2 Command Mode

Context configuration

1.44.3 Syntax Description

This command has no keywords or arguments.

1.44.4 Default

Internal DHCP server functions are disabled for this context.

1.44.5 Usage Guidelines

Use the **dhcp server policy** command to enable internal DHCP server functions in this context and access DHCP server configuration mode.

Note: IP pools on an interface can be used to provide addresses for the DHCP server. If there is no range of values specified on a DHCP subnet, the DHCP server takes the IP addresses from the IP pool defined in the interface command. This IP pool can also be used by the DHCP server and PPP subscribers on the same interface.

Use the **no** form of this command to disable internal DHCP server functions.

1.44.6 Examples

The following example shows how to enable DHCP server functions in the **dhcp** context:

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

1.45 dhcpv6 server (DHCPv6 Policy)

dhcpv6 server

no dhcpv6 server

1.45.1 Purpose

Enables a DHCPv6 server policy and accesses DHCPv6 server policy configuration mode.

1.45.2 Command Mode

Context configuration

1.45.3 Syntax Description

This command has no keywords or arguments.

1.45.4 Default

The DHCPv6 server policy is disabled.

1.45.5 Usage Guidelines

Use the **dhcpv6 server** command in context mode to enable a DHCPv6 server policy for the current context and access DHCPv6 server policy configuration mode.

Only one DHCPv6 server policy is supported for a context. The attributes in a DHCPv6 server policy are applied to subscribers accessing the router through the same context.

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

1.45.6 Examples

The following example shows how to configure a DHCPv6 server policy and access DHCPv6 server policy configuration mode:

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

1.46 dhcpv6 server (Interface)

dhcpv6 server {***ipv6-address*** | ***interface***}

no dhcpv6 server {***ipv6-address*** | ***interface***}

1.46.1 Purpose

Configures an interface to be a DHCPv6 server interface.

1.46.2 Command Mode

Interface configuration

1.46.3 Syntax Description

ipv6-address Specifies the IPv6 address for the DHCPv6 server in the format A:B:C:D::E.

interface Specifies that the DHCPv6 server uses the IPv6 address of the interface in which it is configured.

1.46.4 Default

No DHCPv6 server interface is configured for a context.

1.46.5 Usage Guidelines

Use the **dhcpv6 server** command in interface mode to configure an interface to be a DHCPv6 server interface.

Note: The DHCPv6 server interface must be a last-resort or non-last-resort multibind interface.

Use the **no** form of this command to remove the DHCPv6 server configuration from an interface.

1.46.6 Examples

The following example shows how to configure a multibind last resort interface called **to-red** to be a DHCPv6 server interface; in this case, the server uses the IPv6 address of the interface:

```
[local]Redback(context)#interface to-red multibind lastresort
[local]Redback(config-if)#dhcpv6 server interface
```

1.47 diag on-demand

diag on-demand card slot | standby}[[level lev-num] [loop loop-num]] | [disk disk_num [repair] | [level lev-num] [loop loop-num]]

diag on-demand {**card** *slot* | **standby** [**level** *lev-num*] [**loop** *loop-num*] | **disk** *disk_num* [**repair**] [**level** *lev-num*] [**loop** *loop-num*]}

no diag on-demand card *slot* | **standby** | **disk** *disk_num* **[repair]**

1.47.1 Purpose

Initiates an on-demand diagnostics (ODD) session to test one or more individual chassis units.

1.47.2 Command Mode

exec (10)

1.47.3 Syntax Description

card *slot*	Chassis slot number. Tests the line card, services card, storage card, or standby controller card in the specified slot. The range of values depends on the type of card and the chassis in which the card is installed. For the SmartEdge 100 carrier card, the range of values is 1 to 2; for SmartEdge cards, see the accompanying table for slot range data.
standby	Tests the standby controller card.
disk *disk_num*	Optional. Disk number on the SSE card. Values: 1, 2, all. By default, the rest of the SSE card continues operation while diagnostics run on the specified disk.
level *lev-num*	Optional. Test coverage. The range of values is 1 to 4.
loop *loop-num*	Optional. Number of test iterations. The range of values is 1 to 10.
repair	Optional. Applies only to disks on an SSE card. Attempts to run the repair diagnostic on the specified disk to correct bad data blocks on the file system of the partitions on the disk. The disk must be disabled when the **repair** keyword is specified, but the card must not be disabled. Use this option when the latest result of **diag on-demand** shows that bad blocks are found on one or more of the partitions. The operation typically takes at least 30 minutes per disk to complete.

1.47.4 Default

None

1.47.5 Usage Guidelines

Use the **diag on-demand** command to initiate an ODD session to test one or more individual chassis units.

The ODD tests verify the correct operation of backplane, the standby controller card, the fan and alarm unit (referred to as the fantray) in the SmartEdge 800 chassis, the fan tray and the alarm card in the SmartEdge 400 chassis, and each installed card that has been put in the ODD state. To place a card in the on-demand diagnostic state before initiating an ODD session, see the *General Troubleshooting Guide*.

ODD only runs on disabled components. so you must disable the SSE card or the specified disk on the SSE card, using the **shutdown [disk *disk_num*]** command, before running diagnostics using the **diag on-demand** command. For example, if only disk 1 is disabled (**shutdown disk 1**), when you run the **diag on-demand** command, only disk 1 is diagnosed. The disk must be disabled when you run the **diag on-demand** command with the **repair** keyword, but the card cannot be disabled.

You can test the following cards:

- SmartEdge 100 controller carrier card
- SmartEdge 100 I/O carrier card and media interface cards (MICs)
- Controller cards, when functioning as standby controllers in any other SmartEdge router

  Note: You cannot run ODD on the active controller card in any SmartEdge router.
- 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-48c/STM-16c, and OC-192c/STM-64c line cards
- Advanced Services Engine
- SSE

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

For the SmartEdge 100 chassis, the controller carrier card is in slot 1; the I/O carrier card, including native ports and MICs, is in slot 2.

For a SmartEdge 400 chassis, the standby controller is in slot 5 or 6; for a SmartEdge 600, 800, 1200, or 1200H chassis, the standby controller is in slot 7 or 8.

Table 16 lists the values for the ***slot*** argument for the SmartEdge 400, SmartEdge 600, SmartEdge 800, SmartEdge 1200, and SmartEdge 1200H line cards; in the table, the IR, LR, and SR abbreviations are used for Intermediate Reach, Long Reach, and Short Reach, respectively.

Table 16 Line and Services Card Slots for the diag on-demand Command

Line Card Type and Card Description	***slot*** **Argument Range**		
	SmartEdge 800, 1200, or 1200H Router	**SmartEdge 400 Router**	**SmartEdge 600 Router**
ATM OC-3c/STM-1c (8-port) ATM OC-12c/STM-4c IR (2-port)	1 to 6 and 9 to 14	1 to 4	1 to 6
OC-192c/STM-64c (1-port)	1 to 6 and 9 to 14	1 to 4	1 to 6
Fast Ethernet (60-port) Advanced Gigabit Ethernet (4-port) Gigabit Ethernet 3 (4-port) Gigabit Ethernet 1020 (10-port) Gigabit Ethernet 1020 (20-port) Gigabit Ethernet (5-port) Gigabit Ethernet (20-port) Gigabit Ethernet DDR (10-port) 10 Gigabit Ethernet (1-port) 10 Gigabit Ethernet (4-port) 10 Gigabit Ethernet/OC-192c DDR (1-port)	1 to 6 and 9 to 14	1 to 4	
Advanced Services Engine	1 to 6 and 9 to 14	1 to 4	1 to 6
SmartEdge Storage Engine	1 to 6 and 9 to 14	N/A	1 to 6

Note: The SmartEdge 1200 and 1200H routers do not support all line cards listed in Table 16.

Low-density versions of the line cards are also supported, but only the enabled ports are tested. Use the **`show hardware`** command (in any mode) with the **`card`** and **`detail`** keywords to determine which ports are enabled.

Four levels of tests are supported; Table 17 lists these levels, the types of tests performed, and the units for which the tests are supported.

Table 17 On-Demand Diagnostic Tests

Level	Devices	Tests
1	All	Duplicates the power-on diagnostics (POD) tests Tests completed in 5 to 10 seconds.
2	Standby controller and line cards in SmartEdge routers, controller carrier card, I/O carrier card, and MICs in SmartEdge 100 routers	Includes level 1 tests Tests all on-board active units in the line interface module (LIM) of the board, including memory, registers, Packet Processing ASIC (PPA) Dual Inline Memory Modules (DIMMs) and static RAM (SRAM), PPA and other on-board processors; tests completed in 5 to 10 minutes.
3	Line cards, I/O carrier card, and MICs(1)	Includes level 2 tests Ttests and verifies the card data paths for the entire card with internal loopbacks; tests completed in 10 to 15 minutes.
4	Line cards, I/O carrier card, and MICs(2)	Includes level 3 tests Tests the entire card using external loopbacks; must be run on site with external loopback cables installed.(3)(4)(5)

(1) In addition, the standby controller card only if it is an XCRP4 Controller card.
(2) In addition, the standby controller card only if it is an XCRP4 Controller card.
(3) To run external loopback tests on the Fast Ethernet-Gigabit Ethernet line card, install external loopback plugs on the FE and GE ports. Alternatively, the GE ports can be connected back to back.
(4) To run external loopback tests on the BiDirectional SFPs, install both left and right hand BiDi SFPs. Also BiDi SFPs require explicit cabling between left and right hand ports. The 5-port GE line card is an exception for this ODD test, as it has an extra port. One way to test this extra port is by having two 5-port GE cards in the system.
(5) To run external loopback tests on the Copper SFPs, install external loopback cables between the neighboring ports.

Note: Any MIC, if it is installed, is tested as part of the testing of the I/O carrier card.

Note: If the level you select is not supported for the unit you want to test, the tests run at the highest level for that unit. For example, if you specify level 3 for an XCRP4 Controller card, the system runs the tests at level 2 instead.

Note: To enable or disable POD, enter the **`diag pod`** command in global configuration mode. For more information, see *Managing Hardware*.

Use the **`no`** form of this command to terminate the ODD session.

1.47.6 Examples

The following example shows how to prepare the Ethernet line card in slot **3** for an ODD session and then initiates the session at level **3** with **5** iterations:

```
[local]Redback(config)#card atm-oc3e-8-port 3
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#end
[local]Redback(config-card)#exit
[local]Redback(config)#exit
[local]Redback#diag on-demand card 3 level 3 loop 5
```

The following example shows how an ODD session is initiated at level **2** with **5** iterations for the **standby** controller card:

```
[local]Redback#diag on-demand standby level 2 loop 5
```

The following example shows how to terminate the ODD session:

```
[local]Redback#no diag on-demand standby
```

1.48 diag on-demand mesh

To initiate a packet mesh test the syntax is:

diag on-demand mesh ***slot1 slot2 ... slotn*** **loop** ***loop-num***

no diag on-demand mesh ***slot1 slot2 ... slotn***

To reset the results from all packet mesh tests the syntax is:

diag on-demand mesh reset

1.48.1 Purpose

Initiates a packet mesh test for two or more line cards or resets the results from all packet mesh tests.

1.48.2 Command Mode

exec (10)

1.48.3 Syntax Description

slot1	Slot of the first line card in the mesh that is to be tested. The range of values depends on the type of card and the chassis in which the card is installed; see the accompanying table for slot range data.
slot2	Slot of the second line card in the mesh that is to be tested. The range of values depends on the type of card and the chassis in which the card is installed; see the accompanying table for slot range data.
slotn	Slot of the last line card in the mesh that is to be tested. The range of values depends on the type of card and the chassis in which the card is installed; see the accompanying table for slot range data.
loop ***loop-num***	Number of test iterations. The range of values is 1 to 10.
reset	Resets the results from all packet mesh tests.

1.48.4 Default

None

1.48.5 Usage Guidelines

Use the **diag on-demand mesh** command to initiate a packet mesh test for two or more line cards or to reset the results from all packet mesh tests. The packet mesh test verifies the correct operation of each specified line card (at level 2) and the mesh between cards.

Note: The SmartEdge 100 and SmartEdge 1200/1200H routers do not support this command.

Each specified line card must have been put in the on-demand diagnostics (ODD) state. To place a line card in the ODD state before initiating a packet mesh test, see the hardware guide for your product.

Mesh test results are cumulative; you can run the tests with different slot combinations to help isolate the problem.

You can test the mesh for the following line cards:

- 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-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 the *Card Types* section of the **Configuring Cards** document.

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

Use the **reset** keyword to clear the cumulative results from all mesh tests.

Use the **no** form of this command to terminate the packet mesh test.

To display the results of the level 2 tests that are performed on each card by this command, enter the **show diag** command (in any mode) with the **on-demand** and **card** keywords; to display the results of the mesh test itself, enter the **show diag** command (in any mode) with the **on-demand** and **mesh** keywords.

1.48.6 Examples

The following example shows how to prepare the Ethernet line cards in slot **3** and **4** and initiate a packet mesh test for those cards:

```
[local]Redback#configure
[local]Redback(config)#card fege-60-2-port 3
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#card fege-60-2-port 4
[local]Redback(config-card)#shutdown
[local]Redback(config-card)#on-demand-diagnostic
[local]Redback(config-card)#end
[local]Redback(config-card)#exit
[local]Redback(config)#exit
[local]Redback#diag on-demand mesh 3 4 loop 5
```

1.49 diag pod

diag pod

{**no** | **default**} **diag pod**

1.49.1 Purpose

Enables power-on diagnostics (POD).

1.49.2 Command Mode

Global configuration

1.49.3 Syntax Description

This command has no keywords or arguments.

1.49.4 Default

f

POD tests are enabled.

1.49.5 Usage Guidelines

Use the **diag pod** command to enable power-on diagnostics. Enabling POD takes effect during the next system reload.

Note: To run on-demand diagnostics (ODD), enter the **diag on-demand** command (in exec mode). For information and commands for ODD, see *Managing Hardware*.

The POD tests verify the correct operation of the controller cards, the backplane, fan and alarm unit (referred to as the fan tray in command syntax) in the SmartEdge 800 chassis, the alarm card in the SmartEdge 400 chassis, the fan tray in the SmartEdge 1200 chassis, and each installed line card during a power-on or reload sequence of the SmartEdge router. The tests also run when a controller or line card is installed in a running system. The maximum test time is 130 seconds: 60 seconds for a controller card, 10 seconds for the backplane and fan and alarm unit, or alarm card, and 5 seconds for each installed line card. If the system has two controller cards, the controller tests run in parallel.

During the test duration, the POD tests display results and status; if an error occurs during the testing of a card, the test lights the FAIL LED on the failing card, but does not stop the loading of the operating system. A failure on the

backplane, alarm card, or fan and alarm unit causes the FAN (or FAIL) LED on the fan and alarm unit or alarm card to light.

To display the results of POD tests, enter the **show diag** command in any mode. For more information about this command, see *Managing Hardware*.

Use the **no** form of this command to disable POD tests. Disabling POD tests takes effect during the next system reload.

Use the **default** form to enable power-on diagnostic tests.

1.49.6 Examples

The following example shows how to enable POD tests:

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

The following example shows how to disable the POD tests:

```
[local]Redback(config)#no diag pod
```

1.50 directory

directory [**mate**] [*url*] [{**-size** | **-time**}] [**-reverse**]

1.50.1 Purpose

Displays a list of files in the specified directory on the local file system on either the active or standby controller card.

1.50.2 Command Mode

exec (10)

1.50.3 Syntax Description

mate	Optional. Specifies that the directory is on the controller card to which you are not connected.
url	Optional. URL of the directory with the filenames to be listed; if omitted, uses the current working directory.
-size	Optional. Specifies that the files are displayed in order of size, starting with the smallest.
-time	Optional. Specifies that the files are displayed in order of time, starting with the oldest.
-reverse	Optional. Specifies that files are displayed in reverse order.

1.50.4 Default

Files in the current working directory are displayed in alphabetical order.

1.50.5 Usage Guidelines

Use the **directory** command to display a list of files in the specified directory on the local file system on either the active or standby controller card. The output displays in the same format as the UNIX **ls(1) -l** command.

Use the **mate** keyword to specify the controller card to which you are not connected.

Note: The SmartEdge 100 router does not support standby controller cards; therefore, the **mate** keyword is not applicable.

When referring to a directory on the local file system, the URL takes the following form:

[**/*device***][**/*directory***]...[**/*directory***]

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

1.50.6 Examples

The following example displays a list of files in the root directory of the flash file system:

```
[local]Redback#directory /flash


Contents of /flash
total 44
-rw-r--r--  1 root  0   595 Mar 11 05:24 basic.cfg
drwxr-xr-x  4 root  0   512 Jan 22 07:19 foo
-rw-r--r--  1 root  0  7252 Mar 11 05:24 redback.bin
-rw-r--r--  1 root  0  5454 Mar 11 05:24 redback.cfg
-rw-r--r--  1 root  0  5017 Mar 11 05:24 redback.cfg.bak
drwxr-xr-x  3 root  0   512 Mar 11 05:24 saved
```

1.51 disable

disable

1.51.1 Purpose

Returns the privilege level for the current exec session to the initial privilege level configured for the current administrator account.

1.51.2 Command Mode

exec (10)

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

None

1.51.5 Usage Guidelines

Use the **disable** command to return the privilege level for the current exec session to the initial privilege level configured for the current administrator account. The **no enable** command in exec mode performs the same function. This command is available for any privilege level.

1.51.6 Examples

The following example displays the enable privilege level for the current exec session:

```
[local]Redback#show privilege

Current privilege level is 15
```

The following example returns the current exec session to the initial privilege level for the administrator:

```
[local]Redback#disable
[local]Redback#show privilege level
```

```
The current privilege level is 6
```

1.52 disable (VPLS)

disable

no disable

1.52.1 Purpose

Disables the operation of an enabled Virtual Private LAN Services (VPLS) instance.

1.52.2 Command Mode

VPLS configuration

1.52.3 Syntax Description

This command has no keywords or arguments.

1.52.4 Default

VPLS instances are enabled.

1.52.5 Usage Guidelines

Use the **disable** command to disable the operation of an enabled VPLS instance. When the VPLS instance is disabled, the following actions occur:

- The bridge continues to learn medium access control (MAC) addresses and forwards traffic on all the associated bridge circuits.
- All pseudo-circuits associated with the pseudowires are marked down.

Use the **no** form of this command to enable a previously disabled VPLS instance.

1.52.6 Examples

The following example shows how to disable the VPLS instance on the **to-pe4** bridge:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge to-pe4
[local]Redback(config-bridge)#vpls
[local]Redback(config-vpls)#disable
[local]Redback(config-vpls)#
```

The following example shows how to enable the previously disabled VPLS instance on the **to-pe4** bridge:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#bridge to-pe4
[local]Redback(config-bridge)#vpls
[local]Redback(config-vpls)#no disable
[local]Redback(config-vpls)#
```

1.53 disable-bfd (IS-IS)

disable-bfd

{**no** | **default**} **disable-bfd**

1.53.1 Purpose

Disables Bidirectional Forwarding Detection (BFD) for an Intermediate System-to-Intermediate System (IS-IS) interface.

1.53.2 Command Mode

IS-IS interface configuration

1.53.3 Syntax Description

This command has no keywords or arguments.

1.53.4 Default

BFD is enabled.

1.53.5 Usage Guidelines

Use the **disable-bfd** command to disable BFD for an IS-IS interface.

By default, when BFD is enabled on the same interface on which IS-IS has been enabled, BFD is automatically enabled for each IS-IS neighbor on the interface. When BFD detects a connection failure to an IS-IS neighbor, it notifies IS-IS, and IS-IS sets the neighbor to a down state. If the connection failure persists for more than the IS-IS router dead interval, the IS-IS neighbor is removed. Otherwise, if BFD detects that the connection to the IS-IS neighbor returns, it notifies IS-IS, and IS-IS sets the neighbor to an up state and resumes normal operation. For more information about the IS-IS router dead interval, see the **hello multiplier** command in this document. For more information about BFD, see *Configuring BFD*.

Note: When the **disable-bfd** command is used to disable BFD on an IS-IS interface, all IS-IS neighbors under this particular interface do not respond to BFD messages, but otherwise operate normallyl.

Note: BFD works on a peer-to-peer relationship. A connection failure to one IS-IS neighbor does not affect the status of all other neighbors on the interface.

Use the **no** or **default** form of this command to enable BFD for an IS-IS interface.

1.53.6 Examples

The following example shows how to disable BFD for the IS-IS interface, **foo:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router isis ip-backbone
[local]Redback(config-isis)#interface foo
[local]Redback(config-isis-if)#disable-bfd
[local]Redback(config-isis-if)#
```

1.54 disable-bfd (OSPF)

disable-bfd

{**no** | **default**} **disable-bfd**

1.54.1 Purpose

Disables Bidirectional Forwarding Detection (BFD) for an Open Shortest Path First (OSPF) interface.

1.54.2 Command Mode

OSPF interface configuration

1.54.3 Syntax Description

This command has no keywords or arguments.

1.54.4 Default

BFD is enabled.

1.54.5 Usage Guidelines

Use the **disable-bfd** command to disable BFD for an OSPF interface.

By default, when BFD is enabled on the same interface on which OSPF has been enabled, BFD is automatically enabled for each OSPF neighbor on the interface. When BFD detects a connection failure to an OSPF neighbor, it notifies OSPF, and OSPF sets the neighbor to a down state. If the connection failure persists for more than the OSPF router dead interval, the OSPF neighbor is removed. Otherwise, if BFD detects that the connection to the OSPF neighbor returns, it notifies OSPF, and OSPF sets the neighbor to an up state and resumes normal operation. For more information about BFD, see *Configuring BFD*.

Note: When the **disable-bfd** command is used to disable BFD on an OSPF interface, all OSPF neighbors under this particular interface do not respond to BFD messages, but otherwise operate normally.

Note: BFD works on a peer-to-peer relationship. A connection failure to one OSPF neighbor does not affect the status of all other neighbors on the interface.

Use the **no** or **default** form of this command to enable BFD for an OSPF interface.

1.54.6 Examples

The following example shows how to disable BFD for the OSPF interface, **foo:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#router ospf 15
[local]Redback(config-ospf)#interface foo
[local]Redback(config-ospf-if)#disable-bfd
[local]Redback(config-ospf-if)#
```

1.55 distance (BGP address family)

distance ***external-distance internal-distance local-distance***

{**no** | **default**} **distance** ***external-distance internal-distance local-distance***

1.55.1 Purpose

Configures the administrative distance values for a Border Gateway Protocol (BGP) address family.

1.55.2 Command Mode

BGP address family configuration

1.55.3 Syntax Description

external-distance	Administrative distance for routes external to the autonomous system (AS). The range of values is 1 to 255; the default value is 20.
internal-distance	Administrative distance for routes internal to the AS. The range of values is 1 to 255; the default value is 200.
local-distance	Administrative distance for local routes. The range of values is 1 to 255; the default value is 200. The local distance is the distance assigned to routes that BGP creates using the configuration from the *aggregate address* command.

1.55.4 Default

The external administrative distance is set to 20. The internal and local administrative distances are set to 200.

1.55.5 Usage Guidelines

Use the **distance** command to configure the administrative distance values for a BGP address family. BGP uses distances to compare and prioritize routes. The lower the distance, the more preferred the route.

Use the **no** or **default** form of this command to return the values to their default settings.

1.55.6 Examples

The following example shows how to configure the administrative distance for external routes to **120**, internal routes to **225** and local routes to **5:**

```
[local]Redback(config-bgp-af)#distance 120 225 5
```

1.56 distance (DVSR profiles)

distance *value*

{**no** | **default**} **distance**

1.56.1 Purpose

Configures the distance value for a dynamically verified static routing (DVSR) profile.

1.56.2 Command Mode

DVSR profile configuration

1.56.3 Syntax Description

value	Distance value. The range of values is 1 to 255; the default value is 1.

1.56.4 Default

Distance value is 1, which is the same as static routes.

1.56.5 Usage Guidelines

Use the **distance** command to configure the distance value for a DVSR profile. The distance value is used in the route selection decision.

Note: You can also define the distance value when configuring a DVSR route. In that case, the defined DVSR route distance overwrites the distance specified in the DVSR profile.

Use the **no** or **default** version of this command to reset the distance value in a DVSR profile to the default value of 1.

1.56.6 Examples

The following example shows how to define a DVSR profile using distance of **255:**

```
[local]Redback(config-ctx)#dvsr-profile abc-webfarm
[local]Redback(config-dvsr)#distance 255
```

1.57 distance (IS-IS)

distance ***distance***

{**no** | **default**} **distance**

1.57.1 Purpose

Defines the administrative distance for an Intermediate System-to-Intermediate System (IS-IS) instance.

1.57.2 Command Mode

IS-IS router configuration

1.57.3 Syntax Description

distance	Administrative distance. The range of values is 1 to 255; the default value is 115.

1.57.4 Default

The default administrative distance is 115.

1.57.5 Usage Guidelines

Use the **distance** command to define the administrative distance for an IS-IS instance.

Administrative distance specifies how desirable a route obtained from IS-IS is as compared to the same route obtained from another protocol.

Table 18 lists the default distance for each variety of route sources.

Table 18 Default Distances Per-Route Source

Route Source	Default Distance
connected	0
EBGP	20
OSPF	110
IS-IS	115
RIP	120
IBGP	200

Use the **no** or **default** form of this command to reset the distance value to the default value of 115.

1.57.6 Examples

The following example shows how to modify the administrative distance for the **isis_2** IS-IS instance to **19:**

```
[local]Redback(config-ctx)#router isis isis_2
[local]Redback(config-isis)#distance 19
```

1.58 distance (OSPF)

distance [**external** *distance*] [**inter-area** *distance*] [**intra-area** *distance*]

{**no** | **default**} **distance** [**external** *distance*] [**inter-area** *distance*] [**intra-area** *distance*]

1.58.1 Purpose

Modifies the Open Shortest Path First (OSPF) or OSPF Version 3 (OSPFv3) distance value of one or more route types.

1.58.2 Command Mode

- OSPF router configuration
- OSPF3 router configuration

1.58.3 Syntax Description

external *distance*	Optional. OSPF or OSPFv3 distance for external routes. The range of values is 10 to 255; the default value is 110.
inter-area *distance*	Optional. OSPF or OSPFv3 distance for interarea routes. The range of values is 10 to 255; the default value is 110.
intra-area *distance*	Optional. OSPF or OSPFv3 distance for intraarea routes. The range of values is 10 to 255; the default value is 110.

1.58.4 Default

Each distance is set to 110.

1.58.5 Usage Guidelines

Use the **distance** command to modify the OSPF or OSPFv3 distance value of one or more route types. OSPF and OSPFv3 use distances to compare and prioritize routes. The lower the distance, the more preferred the route. When you enter this command without any optional keywords, the distance for all route types are set to 110.

Use the **no** or **default** form of this command to return the values to their default settings.

1.58.6 Examples

The following example shows how to set the OSPF distance for external routes to **120:**

```
[local]Redback(config-ospf)#distance external 120
```

1.59 distance (RIP)

distance ***distance***

{**no** | **default**} **distance**

1.59.1 Purpose

Modifies the administrative distance for the Routing Information Protocol (RIP) or RIP next generation (RIPng) instance.

1.59.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.59.3 Syntax Description

distance	Administrative distance. The range of values is 1 to 255; the default value is 120.

1.59.4 Default

The administrative distance is 120.

1.59.5 Usage Guidelines

Use the **distance** command to modify the administrative distance for the RIP or RIPng instance.

Administrative distance specifies how desirable a route obtained from RIP or RIPng is compared to the same route obtained from another protocol. The lower the value for the ***distance*** argument in comparison to other routes obtained from other protocols, the more desirable the RIP or RIPng route becomes.

Use the **no** or **default** form of this command to return the administrative distance to the default value of 120.

1.59.6 Examples

The following example shows how to set the administrative distance for the **rip001** RIP instance to **200:**

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#distance 200
```

1.60 distribute-list

distribute-list prefix *pl-name* {**in** | **out**} [*if-name*]

no distribute-list prefix *pl-name* {**in** | **out**} [*if-name*]

1.60.1 Purpose

Applies a prefix list to Routing Information Protocol (RIP) or RIP next generation (RIPng) packets.

1.60.2 Command Mode

- RIPng router configuration
- RIP router configuration

1.60.3 Syntax Description

prefix *pl-name*	Name of the prefix list to be applied to RIP or RIPng packets.
in	Applies the prefix list to incoming RIP or RIPng updates.
out	Applies the prefix list to outgoing RIP or RIPng updates.
if-name	Optional. Name of the interface to which the prefix list is applied.

1.60.4 Default

Prefix lists are not applied.

1.60.5 Usage Guidelines

Use the **distribute-list** command to apply a prefix list to RIP or RIPng packets.

Use the **no** form of this command to remove a prefix list from RIP or RIPng packets.

1.60.6 Examples

The following example shows how to apply the prefix list, **list1**, to incoming updates from the **fe01** interface:

```
[local]Redback(config-ctx)#router rip rip001
[local]Redback(config-rip)#distribute-list prefix list1 in fe01
```

1.61 dnis generate

dnis generate

{**no** | **default**} **dnis**

1.61.1 Purpose

Directs the Layer 2 Tunneling Protocol (L2TP) process to transmit the Calling-Number AVP (22) in Incoming-Call-Requests (ICRQs).

1.61.2 Command Mode

L2TP peer configuration

1.61.3 Syntax Description

This command has no keywords or arguments.

1.61.4 Default

The transmission of the Calling-Number AVP in the ICRQ is disabled.

1.61.5 Usage Guidelines

Use the **dnis generate** command to direct the Layer 2 Tunneling Protocol (L2TP) process to transmit the Calling-Number AVP (22) in Incoming-Call-Requests (ICRQs). Use this command only when the SmartEdge router is acting as a LAC.

You can use the **l2tp avp calling-number format** command in context configuration mode to control the value of the Calling-Number AVP.

Use the **no** or **default** form of this command to disable transmission of the Calling-Number AVP in ICRQs.

1.61.6 Examples

The following example shows how to enable the L2TP process to transmit the Calling-Number AVP (22) in the ICRQ:

```
[local]Redback(config-l2tp)#dnis generate
```

1.62 dns

dns {**primary** | **secondary**} ***ip-addr***

no dns {**primary** | **secondary**} ***ip-addr***

1.62.1 Purpose

Configures the IPv4 address of a primary (and, optionally, secondary) Domain Name System (DNS) server for a subscriber.

1.62.2 Command Mode

Subscriber configuration

1.62.3 Syntax Description

primary	Configures the IPv4 address of a primary DNS server.
secondary	Configures the IPv4 address of a secondary DNS server.
ip-addr	DNS server IP address.

1.62.4 Default

No DNS servers are preconfigured.

1.62.5 Usage Guidelines

Use the **dns** command to configure the IPv4 address of a primary (and, optionally, secondary) DNS server for a subscriber.

Use the **no** form of this command to remove the DNS server information from a subscriber record.

1.62.6 Examples

The following example shows how to configure a primary DNS server address of **10.2.3.4** for subscriber, **kenny:**

```
[local]Redback(config-ctx)#subscriber name kenny
[local]Redback(config-sub)#dns primary 10.2.3.4
```

1.63 dns6

dns6 {**primary** | **secondary**} ***ip-addr***

no dns6 {**primary** | **secondary**} ***ip-addr***

1.63.1 Purpose

In a subscriber record or profile, configures the IPv6 address of a primary (and, optionally, secondary) Domain Name System (DNS) server for a subscriber.

1.63.2 Command Mode

- Default subscriber profile configuration
- Subscriber record configuration
- Subscriber profile configuration

1.63.3 Syntax Description

primary	Configures the IPv6 address of a primary DNS server.
secondary	Configures the IPv6 address of a secondary DNS server.
ip-addr	DNS server IPv6 address.

1.63.4 Default

No IPv6 DNS servers are preconfigured

1.63.5 Usage Guidelines

Use the **dns6** command to configure the IPv6 address of a primary (and, optionally, secondary) DNS server for a subscriber.

Use the **no** form of this command to remove the DNS server information from a subscriber record

1.63.6 Examples

The following example shows how to configure a primary DNS server IPv6 address of **2001:db:b:4f::2** for the subscriber called **kenny:**

```
[local]Redback(config-ctx)#subscriber name kenny
[local]Redback(config-sub)#dns6 primary 2001:db:b:4f::2
```

1.64 domain (context)

domain ***alias*** [**advertise**]

no domain ***alias*** [**advertise**]

1.64.1 Purpose

Creates a unique domain alias for the current context for use in subscriber authentication.

1.64.2 Command Mode

Context configuration

1.64.3 Syntax Description

alias	Domain alias for the current context. The domain alias can include a single wildcard. The default wildcard character is an asterisk (*). See the **service domain-wildcard** command for information on configuring wildcard characters.
advertise	Optional. Advertises the domain alias in Point-to-Point Protocol over Ethernet (PPPoE) discovery messages.

1.64.4 Default

No domain aliases are created.

1.64.5 Usage Guidelines

Use the **domain** command in context configuration mode to create a domain alias for the current context for use in subscriber authentication. This command provides a flexible way to associate subscribers with contexts. With the exception of wildcard domain aliases, whose use is restricted to subscriber authentication, you can use a domain alias instead of a context name in any command that takes a context name as an argument.

You can create any number of aliases; however, each alias must be unique across all contexts.

When one or more domain aliases are configured with this command, a subscriber can authenticate as ***username@ctx-name*** or ***username@alias*** and, in either case, be associated with the same context.

Table 19 provides the rules used when matching domain aliases with embedded wildcards to subscriber logins:

Table 19 Rules Governing Matching Aliases to Subscriber Logins:

Rule	Description
wildcards allowed: per domain alias	Only one wildcard character (*) can be specified in each domain alias.
wildcard matching: to multiple characters	A wildcard can match multiple contiguous characters or no characters; for example, “bob*” matches both “bobby” and “bob.”
domain alias: uniqueness	You are not allowed to define a domain alias with an embedded wildcard if the domain alias name matches an existing context or domain alias name. An example is provided in Section 1.64.6 on page 132.
first criteria: far left characters	When a subscriber log-in name matches more than one wildcard domain, the far left characters have the highest matching significance. An example is provided in Section 1.64.6 on page 132.
second criteria: number of characters	If a subscriber log-in name matches more than one wildcard domain and a priority cannot be chosen on the basis of the far left characters, the subscriber is associated with the context whose domain alias provides the greatest number of matching characters. In Section 1.64.6 on page 132, the subscriber sub@RBAKERICemployee.com would be associated with the context bar rather than the context bob because RBAKERICemployee.com matches **RBAKERIC*** (bar) in eight characters while matching **RB*** (bob) in only two characters.

Use the **no** form of this command to delete the domain alias.

For additional information, see *Configuring Service Policies*.

1.64.6 Examples

The following example shows how to create a domain alias, **guest**, for the **isp1** context and advertise it in PPPoE discovery messages:

```
[local]Redback(config)#context isp1
[isp1]Redback(config-ctx)#domain guest advertise
```

In the following example, the domain alias **bar*** is not allowed because it matches the already existing context **bar:**

```
[local]Redback(config)#context bar
[local]Redback(config-ctx)#domain RBAKERIC*
[local]Redback(config-ctx)#domain *com
[local]Redback(config-ctx)#domain bar*
Error: This name is already a domain or context name
```

In the following example, **user@RBAKnetworks.com** matches the domain aliases **RBAK*** and ***com**. The user would be associated with the context **bob** because of the priority given to far left characters:

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

[local]Redback(config-ctx)#domain RBAKERIC*

[local]Redback(config-ctx)#domain *com

[local]Redback(config-ctx)#commit

[local]Redback(config-ctx)#exit

[local]Redback(config)#context bob

[local]Redback(config-ctx)#domain RB*

[local]Redback(config-ctx)#domain bob*bar

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

1.65 domain (L2TP peer)

domain ***alias***

no domain ***alias***

1.65.1 Purpose

Assigns a domain alias to a Layer 2 Tunneling Protocol (L2TP) peer or group.

1.65.2 Command Mode

- L2TP peer configuration
- L2TP group configuration

1.65.3 Syntax Description

alias	Unique name to be used as an alias. Must be one of the domain aliases created for the context in which the peer is being configured by the **domain** command in context configuration mode.

1.65.4 Default

No aliases are specified.

1.65.5 Usage Guidelines

Use the **domain** command to assign a domain alias for a peer; the domain alias is one previously created for the context in which the L2TP peer or group is configured.

Note: To create an alias for a context, use the **domain** command in context configuration mode. For more information, see the *Configuring Contexts and Interfaces*.

A domain alias can be a simpler name (for example, isp.net) than its name (the ***l2tp-peer-name*** argument specified by the **l2tp-peer** command in L2TP peer configuration mode), which is a fully qualified domain name, such as time_0_5.chi_core.isp.net. You can specify multiple aliases for each L2TP peer or group.

You can use a domain alias for a peer anywhere that you can use its name (the ***l2tp-peer-name*** argument) or for a group anywhere that you can use its name (the ***l2tp-group-name*** argument specified by the **l2tp-group** command in L2TP group configuration mode). You cannot use this command if you entered

L2TP peer configuration mode using the **l2tp-peer** command in context configuration mode with the **default** keyword.

Use the **no** form of this command to remove the specified domain alias.

1.65.6 Examples

The following example shows how to select (or create) an L2TP peer and assign a domain alias for it:

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

The following example shows how to select (or create) an L2TP group and assign a domain alias for it:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#domain field-sales
[local]Redback(config-ctx)#l2tp-group name group1
[local]Redback(config-l2tp-group)#domain field-sales
```

1.66 domain-name

domain-name ***domain-name***

no domain-name

1.66.1 Purpose

Names a maintenance domain (MD).

1.66.2 Command Mode

CFM configuration

1.66.3 Syntax Description

domain-name	The name used to identify the MD to CFM users who have access to the current MD level. The total length of MD name (***domain-name*** argument) and the MA short-name must be less than or equal to 45 characters.

1.66.4 Default

The default MD name is the same as the CFM instance name set by the **ethernet-cfm** command.

1.66.5 Usage Guidelines

Use this command to name an MD.

A maintenance domain can be thought of as a collection of maintenance points visible at a specific MD level through domain service access points (DSAPs).

You can configure the SmartEdge router Ethernet ports and circuit interfaces into multiple MDs, but each MD must have its own unique name. MDs in the SmartEdge router can be nested or adjacent, but intersecting domains are not allowed.

Adjacent (touching) MDs occur when two or more MDs link to each other through an Ethernet bridge. Nested domains are used in situations where a customer or service provider does not maintaining all the Ethernet nodes they use. The maintenance of these nodes is given to CFM lower level MDs. Each domain in a nested set has its own MD level; typically, a customer has the highest MD level, service providers at lower MD level, and device operators at the lowest MD levels. See the following figure:

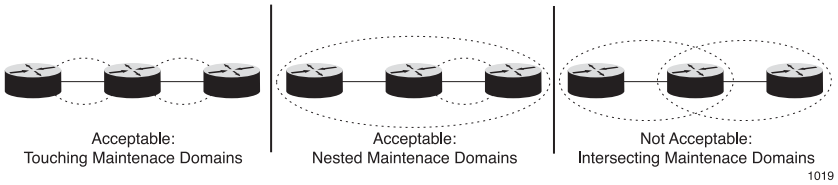

Figure 1 MD Levels

The following drawing illustrates nested domains. The Service Provider domain is nested in the Customer Domain, and two Operator domains are nested in the Service Provider domain:

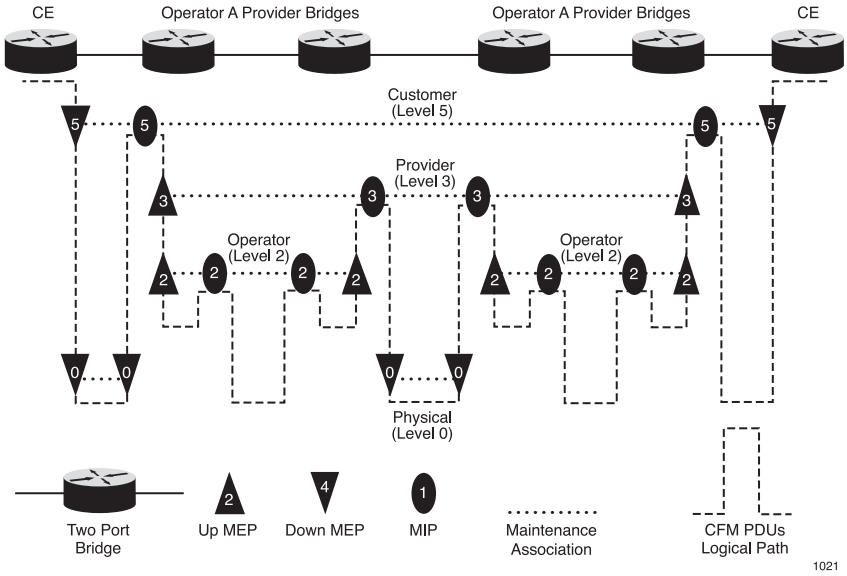

Figure 2 Nested Domains

1.66.6 Examples

The following example shows how to use this command to create the maintenance instance **instance-1** and the maintenance domain named **sbc.com** at MD level 4:

```
[local]Redback(config)#ethernet-cfm instance-1

[local]Redback(config-ether-cfm)#level 4

[local]Redback(config-ether-cfm)#domain-name sbc.com
```

1.67 dot1q profile

dot1q profile ***prof-name***

no dot1q profile ***prof-name***

1.67.1 Purpose

Creates a new 802.1Q profile or selects an existing one for modification, and enters dot1q profile configuration mode.

1.67.2 Command Mode

Global configuration

1.67.3 Syntax Description

prof-name	Alphanumeric string to be used as the name of the particular profile.

1.67.4 Default

No 802.1Q profiles are defined.

1.67.5 Usage Guidelines

Use the **dot1q profile** command to create a new 802.1Q profile or to select an existing profile for modification, and to enter dot1q profile configuration mode.

Note: You must create an 802.1Q profile before you can configure 802.1Q permanent virtual circuits (PVCs) that reference the profile name.

Use the **no** form of this command to delete an 802.1Q profile. This form deletes any PVCs that reference that profile.

1.67.6 Examples

The following example shows how to create an 802.1Q profile, **dot1q-pro**, and enters dot1q profile configuration mode:

```
[local]Redback(config)#dot1q profile dot1q-pro
[local]Redback(config-dot1q-profile)#
```

1.68 dot1q pvc

In link group or port configuration mode, to create or select an 802.1Q tunnel and allow the creation of inner PVC in the tunnel:

dot1q pvc *tunl-vlan-id* **[profile** *prof-name***] encapsulation 1qtunnel [replicate]**

no dot1q pvc *tunl-vlan-id*

In link group or port configuration mode, to create or select a range of static 802.1Q PVCs:

dot1q pvc [explicit] *start-vlan-id* **[through** *end-vlan-id***] [profile** *prof-name***] [encapsulation** *encaps-type***] [replicate]**

no dot1q pvc [explicit] *start-vlan-id* **[through** *end-vlan-id***]**

In link group or port configuration mode, to create or select a range of static 802.1Q PVCs within a tunnel:

dot1q pvc [explicit] *tunl-vlan-id*:*start-vlan-id* **[through** *end-vlan-id***] [profile** *prof-name***] [encapsulation** *encaps-type***] [replicate]**

no dot1q pvc [explicit] *tunl-vlan-id*:*start-vlan-id* **[through** *end-vlan-id***]**

In link group mode or port configuration mode, to create or select a range of on-demand 802.1Q PVCs:

dot1q pvc on-demand *start-vlan-id* **[through** *end-vlan-id***] [[profile** *prof-name***] [encapsulation** *encaps-type***] | {aaa context** *ctx-name* **| aaa context [prefix-string** *text* **| user-name** *subscriber***]}] [replicate]**

no dot1q pvc on-demand *start-vlan-id*

In link group or port configuration mode, to create or select a range of on-demand 802.1Q PVCs within a tunnel:

dot1q pvc on-demand ***tunl-vlan-id*****:*****start-vlan-id*** **[through** ***end-vlan-id*****] [profile** ***prof-name*****] [encapsulation** ***encaps-type*****] [replicate]**

no dot1q pvc on-demand ***tunl-vlan-id*****:*****start-vlan-id***

In port configuration mode, to create or select one or more transport-enabled 802.1Q PVCs on an Ethernet port or in an 802.1Q tunnel on an Ethernet port, see Section 1.69 on page 147.

dot1q pvc transport...

1.68.1 Purpose

Creates or selects an 802.1Q PVC and enters the PVC configuration mode.

1.68.2 Command Mode

- Link group configuration
- Port configuration

1.68.3 Syntax Description

tunl-vlan-id	802.1Q virtual LAN (VLAN) tag value for the 802.1Q tunnel. The range of values is 1 to 4095.
start-vlan-id	First 802.1Q VLAN tag value for a range of PVCs to be configured. The range of values is 1 to 4095.
through ***end-vlan-id***	Optional. Last 802.1Q VLAN tag value for a range of PVCs to be configured.
profile ***prof-name***	Optional. Existing 802.1Q profile. The dot1q profile that you specify must exist before you enter this command.

encapsulation ***encaps-type***	Optional. Encapsulation, according to one of the following keywords:(1) • **1qtunnel**—Specifies that the PVC is a tunnel. A tunnel allows the creation of inner PVCs in the tunnel. • **multi**—Enables multiprotocol encapsulation (the creation of a child circuit), and enters the dot1q pvc configuration mode where the protocol of the child circuit is set through the **circuit protocol** command. • **pppoe**—Specifies Point-to-Point Protocol over Ethernet (PPPoE) encapsulation. • **raw**—Specifies raw mode. Raw encapsulation mode strips the Layer 2 headers from the packet and allows switching raw encapsulation mode packets without Layer 2 processing. See *Configuring Cross-Connections* for further information on the applications of raw encapsulation PVCs. This option is intended for 802.1Q tunnels or static 802.1Q PVCs; does not apply to on-demand PVCs. This option allows you to cross-connect an 802.1Q tunnel or a PVC to another 802.1Q tunnel or PVC.(2) If this option is not specified, the default encapsulation is IP over Ethernet (IPoE).
explicit	Optional. Specifies that the configuration for the individual PVCs in the range of static PVCs is not expanded in the configuration file. This keyword has no affect on the functionality of the PVCs, but only on whether their configuration is stored as a range or individually.

on-demand	Specifies an on-demand (listening) PVC or a range of on-demand PVCs; an on-demand PVC is created in memory only after traffic is detected on it. On-demand PVCs can exist on an Ethernet port or 802.1Q tunnel. • You can configure on-demand PVCs on an Ethernet port or within an 802.1Q tunnel. • L2VPN cross connections (XC) configured with on-demand 802.1q PVCs are not supported. • You cannot configure overlapping transport ranges (with the exception of the fallback transport range [keyword `any`]) or overlapping circuit creation-on demand (CCOD) ranges. In addition, overlapping transport and CCOD ranges are not allowed.
aaa	Specifies that the 802.1Q PVCs are created using Remote Authentication Dial-In User Service (RADIUS).
context ***ctx-name***	Name of the context in which the RADIUS servers are configured for AAA configurations.
prefix-string ***text***	String to be used as a prefix in the generation of the name of the subscriber record in RADIUS. The string must not contain spaces, periods, underscores, or forward or backward slashes.
user-name ***subscriber***	String to be used for the exact name of the subscriber record in RADIUS, in any valid structured subscriber name format; it can be up to 253 characters.

replicate	Optional. Replicates features of the PVC. Only 802.1Q tunnel encapsulation is currently supported for replication: • When an outer PVC pseudocircuit in a link group is configured with the **replicate** keyword, but its inner PVCs are not, the features of the outer PVC are replicated and distributed on the other active ports in the group, while the features of the inner PVCs are replicated on one of the other active ports in the link group, but not distributed. • Replication of the inner PVCs is not supported. If an outer PVC pseudocircuit in a link group and its inner PVCs are configured with the **replicate** keyword, the features of the inner and outer PVC are both replicated and distributed on the other active ports in the link group.
transport	See the **dot1q pvc transport** command in Section 1.69 on page 147.

(1) You cannot change the encapsulation of an 802.1Q PVC unless you first delete it and then recreate it.
(2) The `raw` keyword is not available for 802.1Q PVCs in link group configuration mode.

1.68.4 Default

No 802.1Q PVCs or tunnels are defined.

1.68.5 Usage Guidelines

Use the **dot1q pvc** command to create or select an 802.1Q PVC and enter the PVC configuration mode. The PVCs can be on an Ethernet port, or under an access link group or in an 802.1Q tunnel under an access link group

When entered in link group configuration mode, this command creates or selects an aggregated 802.1Q tunnel or a PVC in the link group. When an Ethernet port is added to the link group, an 802.1Q tunnel or a PVC with that ***vlan-id*** tag is created on that port.

Note: You cannot create 802.1Q PVCs or tunnels on the Ethernet management port on a controller card.

Many 802.1Q implementations use VLAN tag value 1 as a management PVC. To ensure interoperability, we recommend that you do not use VLAN tag value 1 for non-management traffic.

You cannot specify the same VLAN tag value for an 802.1Q tunnel and an 802.1Q PVC that is not configured within the tunnel.

Use the **through** ***end-vlan-id*** construct to create or select groups of similar PVCs on an Ethernet port. The following guidelines apply when you use the **through** keyword:

- Any 802.1Q PVCs in the specified range that do not already exist are created with the specified profile and encapsulation.
- Any 802.1Q PVCs in the specified range that already exist and do not have the specified encapsulation cause the command to fail; you must delete these PVCs and then enter the **dot1q pvc** command again.
- When you use the no form of this command with the through keyword, all 802.1Q PVCs in the range are deleted, regardless of whether those PVCs have the same profile and encapsulation.

The **multi** keyword applies to 802.1Q PVCs that have child circuits. The parent 802.1Q PVC carries IPoE traffic. To create child circuits on multi-encapsulated 802.1Q PVCs, use the **circuit protocol** command (in dot1q PVC configuration mode); to cross-connect them, see *Configuring Cross-Connections*. The child circuit usually carries PPPoE traffic.

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

Use the **no** form of the **dot1q pvc** or **dot1q pvc on-demand** command to delete an 802.1Q PVC or tunnel. If you delete a tunnel, all 802.1Q PVCs configured within that tunnel are also deleted.

1.68.6 Examples

The following example shows how to create an 802.1Q PVC with the VLAN tag value **20** on Ethernet port **3/1:**

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 20
[local]Redback(config-dot1q-pvc)#
```

The following example shows how to create two 802.1Q PVCs with tag values **26** and **27** for two aggregated 802.1Q PVCs in the link group **lg1:**

```
[local]Redback(config)#link-group lg1 dot1q
[local]Redback(config-link-group)#dot1q pvc 26
[local]Redback(config-link-pvc)#exit
[local]Redback(config-link-group)#dot1q pvc 27
[local]Redback(config-link-pvc)#exit
```

The following example shows how to create an 802.1Q tunnel with the VLAN tag value **30** and an 802.1Q PVC with the VLAN tag value **100** within it:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 30 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 30:100 encapsulation multi
[local]Redback(config-dot1q-pvc)#exit
```

The following example shows how to create an 802.1Q tunnel with the VLAN tag value **30** and a range of on-demand 802.1Q PVCs with VLAN tag values **100** through **200** within it:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 30 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc on-demand 30:100 through 200 encapsulation pppoe
[local]Redback(config-port)#bind authentication chap
[local]Redback(config-dot1q-pvc)#exit
```

The following example shows how to create the inner VLAN **100:200** of type **raw** under the tunnel VLAN **100:**

```
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-dot1q)#dot1q pvc 100 encapsulation 1qtunnel
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 100:200 encapsulation raw
```

1.69 dot1q pvc transport

```
dot1q pvc transport {any | [tunl-vlan-id:] {any |
start-vlan-id [through end-vlan-id]}} [profile prof-name]

no dot1q pvc transport {any | [tunl-vlan-id:] {any |
start-vlan-id [through end-vlan-id]}}
```

1.69.1 Purpose

Creates or selects a transport-enabled 802.1Q PVC and enters the PVC configuration mode.

1.69.2 Command Mode

- Port configuration
- Link group configuration

1.69.3 Syntax Description

any	Optional. Specifies a fallback transport range for all traffic not assigned to a PVC or another transport range. The implicit VLAN boundary is from 1 to 4095.(1)
tunl-vlan-id	Optional. 802.1Q virtual LAN (VLAN) tag value for the 802.1Q tunnel. The range of values is 1 to 4095.(2)
start-vlan-id	Optional. First 802.1Q VLAN tag value for a range of PVCs. The range of values is 1 to 4095.(1)(2)
through ***end-vlan-id***	Optional. Last 802.1Q VLAN tag value for a range of PVCs.(1)(2)
profile ***prof-name***	Optional. Existing 802.1Q profile.

(1) The term transport range means the range of VLAN IDs that are transport-enabled by the `dot1q pvc transport` *command.*
(2) Restrictions to the configuration of transport ranges are found in Table 20.

1.69.4 Default

No transport-enabled 802.1Q PVCs or tunnels are defined.

1.69.5 Usage Guidelines

Use the **dot1q pvc transport** command to create or select a transport-enabled 802.1Q PVC and enter the PVC configuration mode. The

transport-enabled PVCs can be on an Ethernet port, or under an access link group or in an 802.1Q tunnel under an access link group.

Use the **no** form of the **dot1q pvc transport** command to delete the transport range and disable the transport of packets with VLAN IDs in the associated range.

A transport-enabled PVC is like a normal 802.1Q PVC but with four key differences:

- A transport-enabled 802.1Q PVC is a circuit where some or all of the VLAN tagging may be carried intact across the Layer-2 entity to which the circuit is bound.

- The only entities that can be bound to a transport-enabled 802.1Q PVC are L2VPN cross connections, VPLS bridges, and non-VPLS bridges.

- In a transport-enabled 802.1Q PVC, the keyword `any` can be used instead of a specific inner or outer VLAN ID or range of IDs.

  – When the `any` keyword is applied to a port or link-group, it creates a catch-all fallback range; that is, it transport-enables all 802.1Q PVCs in the port or link-group that are not otherwise specified.

  – When the `any` keyword is applied to a 1q tunnel, it creates a catch-all fallback range for PVCs in the tunnel; that is it-transport enables all 802.1Q PVCs in the tunnel that are not otherwise specified.

- PVCs using a range of VLAN values, or the `any` keyword, are represented internally as a single circuit, compared to non-transport circuits which are represented with separate circuits for each VLAN ID.

1.69.5.1 Restrictions

Table 20 provides the restrictions that apply to the **dot1q pvc transport** command.

Table 20 dot1q pvc transport Command Restrictions

Restriction	Description
VLAN tag value 1	Many 802.1Q implementations use VLAN tag value 1 as a management PVC. To ensure interoperability, we recommend that you do not use VLAN tag value 1 for non-management traffic.
Management port of controller card	You cannot create 802.1Q PVCs or tunnels on the Ethernet management port on a controller card.

Table 20 dot1q pvc transport Command Restrictions

Restriction	Description
through ***end-vlan-id***	Use the **through** ***end-vlan-id*** construct to create or select groups of similar PVCs on an Ethernet port. The following guidelines apply when you use the **through** keyword: • Any 802.1Q PVCs in the specified range that do not already exist are created with the specified profile and encapsulation. • When you use the **no** form of this command with the **through** keyword, existing non-transport PVCs with VLAN IDs that fall in the range are not deleted. • You cannot configure overlapping transport ranges (with the exception of the fallback transport range [keyword `any`]) or overlapping circuit creation-on demand (CCOD) ranges. In addition, overlapping transport and CCOD ranges are not allowed.
propagation commands	Propagation commands configured under a parent 802.1Q PVC with **1q tunnel** encapsulation apply to any child transport range. In this case, the 802.1p value from the outer PVC header is used for propagation and value mappings. Propagation commands configured under a child transport range override any propagation settings specified for the parent 802.1Q PVC. In this case, the 802.1p value from the inner PVC header is used for propagation and value mappings. If a profile is specified, only the **propagate from qos**, **propagate to qos**, and **propagate qos transport use-vlan-header** commands apply to this usage of the command. Each transport range can specify a different classification map for propagation. Only propagation references defined in the 802.1Q profile are used.
Bindings	The bound entity can only be an L2VPN, a VPLS bridge, or a non-VPLS bridge. No other types of bindings are supported. After binding, only the **shutdown** command and its **no** form can be applied to the transport range. When the transport range, parent port, or 802.1Q tunnel is shut down, traffic is dropped.

1.69.5.2 Simple Bridge with Transport-Enabled Circuits

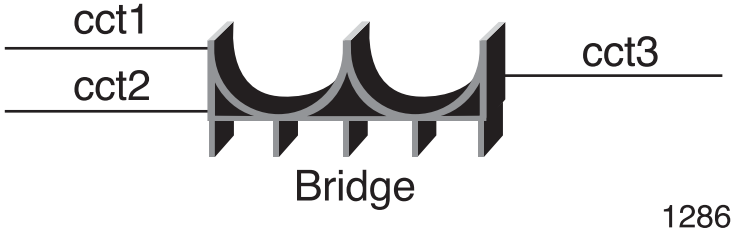

Figure 3 Simple Bridge with Transport-Enabled Circuits

The preceding illustration shows how transport-enabled circuits (cct1, cct2, and cct3) can be used to transport Dot1Q packets across a simple bridge (non-VPLS) configured in a context.

In a very simple scenario, the endpoints of cct1, cct2, and cct3 could be customer equipment connected on a number of VLANs that pass through the bridge. Because the circuits bound to the bridge are transport enabled, the VLAN tags can be passed intact through the bridge.

1.69.5.3 L2VPN Cross-Connect (or VPLS Configuration) with Transport-Enabled Circuits

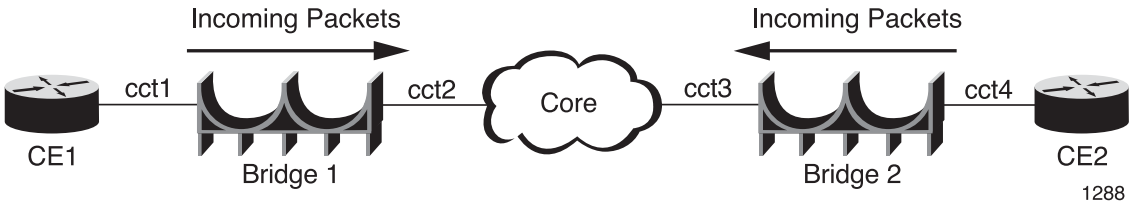

Figure 4 L2VPN Cross-Connect (or VPLS Configuration) with Transport-Enabled Circuits

The preceding figure shows how transport-enabled circuits can be used.

- cct1 and cct4 are transport-enabled attachment circuits bound to a VPLS-bridge or L2VPN.
- cct2 and cct3 are MPLS-enabled L3 interfaces.

Up to three VLAN tags can be transported across a VPLS-bridge or an L2VPN cross-connect. The following tables show how VLAN tags are treated within a VPLS-bridge for various **`dot1q pvc transport`** configurations.

Table 21 VLAN Tags and VPLS: transport A to transport B

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A**	**Within the VPLS Bridge**	**Egress at Bridge 2 on cct4** **dot1q pvc transport B**
1	A	A	B
2	A:X	A:X	B:X
3	A:X:Y	A:X:Y	B:X:Y

Table 22 VLAN Tags and VPLS: transport A:any to transport B:any

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A:any**	**Within the VPLS Bridge**	**Egress at Bridge 2 on cct4** **dot1q pvc transport B:any**
1	A (packet processed on the parent circuit)	N/A	N/A
2	A:X	A:X	B:X

Table 22 VLAN Tags and VPLS: transport A:any to transport B:any

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A:any**	**Within the VPLS Bridge**	**Egress at Bridge 2 on cct4** **dot1q pvc transport B:any**
3	A:X:Y	A:X:Y	B:X:Y
4	A:X:Y:Z	A:X:Y:Z	B:X:Y:Z

Table 23 VLAN Tags and VPLS: transport A:B to transport C:B

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A:B**	**Within the VPLS Bridge**	**Egress at Bridge 2 on cct4** **dot1q pvc transport C:B**
1	A:B	A:B	C:B
2	A:B:X	A:B:X	C:B:X

Table 24 VLAN Tags and VPLS: transport any to transport any

	Ingress at Bridge 1 on cct1 **dot1q pvc transport any**	**Within the VPLS Bridge**	**Egress at Bridge 2 on cct4** **dot1q pvc transport any**
1	A	A	A
2	A:B	A:B	A:B
3	A:B:C	A:B:C	A:B:C

The following tables show how VLAN tags are treated within an L2VPN cross-connect for various **`remote-encap`** configurations.

Table 25 VLAN Tags and L2VPN When remote-encap = dot1q

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A**	**Within L2VPN**	**Egress at Bridge 2 on cct4** **dot1q pvc transport B**
1	A	A	B
2	A:X	A:X	B:X
3	A:X:Y	A:X:Y	B:X:Y

Table 26 VLAN Tags and L2VPN When remote-encap = ethernet

	Ingress at Bridge 1 on cct1 **dot1q pvc transport A**	**Within L2VPN**	**Egress at Bridge 2 on cct4** **dot1q pvc transport B**
1	A	Untagged	B
2	A:X	X	B:X
3	A:X:Y	X:Y	B:X:Y

1.69.6 Examples

1.69.6.1 Example of Matching Criteria for Incoming Packets

The following example shows L2VPN cross-connection and VPLS bridge entities bound to transport-enabled PVCs and shows how the L2 tags of incoming packets are handled after the best-match has been determined.

When an incoming packet arrives at an 802.1Q encapsulated port, the port determines on which circuit the packet is arriving, so that the port can send the packet to the best-matched binding entity for handling. The packet is always handled by the best-match circuit.

Once a PVC has been matched, the packet is handled by the entity bound to that PVC. If there is nothing bound to that PVC, the packet is dropped.

Which VLAN tags, if any, are retained during transport depend on how the L2 entity and transport circuits bound to the entity are configured.

Note: The keyword `any` matches any single or double-tagged packet; however the tags that are transported across the L2VPN depends on the configured value of `remote-encap` and in the case of VPLS configurations, the tags transported depend on the dummy tag configured for the pseudowire.

```
context local
!
 l2vpn

 xc-group My_L2VPN
!  LDP circuit bindings
   xc 3/4 vlan-id any transport vc-id 1 peer 2.2.2.2
   xc 3/4 vlan-id 100 transport vc-id 2 peer 2.2.2.2
   xc 3/4 vlan-id 101:100 through 200 transport vc-id 3 peer 2.2.2.2
   xc 3/4 vlan-id 102 : any transport vc-id 4 peer 2.2.2.2

port ethernet 3/4
 no shutdown
 encapsulation dot1q

 ! create PVC that matches "any." See note for further information
 dot1q pvc transport any
  l2vpn local

 ! create PVC that matches single or double-tagged packet with outer tag 100
 ! transport all tags across L2VPN
 dot1q pvc transport 100
  l2vpn local

 ! create PVC that matches double-tagged packet with outer tag 101
 ! and inner tag 100-200
 ! transport both tags across L2VPN
 dot1q pvc 101 encapsulation 1qtunnel
  dot1q pvc transport 101:100 through 200
   l2vpn local

 ! create PVC that matches double-tagged packet with outer tag 102,
 ! transport both tags across L2VPN
 dot1q pvc 102 encapsulation 1qtunnel
  dot1q pvc transport 102:any
   l2vpn local

 ! create PVC that matches single or double-tagged packet with
 ! outer tag 200
 ! transport all tags across VPLS
 dot1q pvc transport 200
  bind interface my_vpls_bridge local

 ! create PVC that matches double-tagged packet with outer tag 201,
 ! transport inner tag across VPLS
 dot1q pvc 201 encapsulation 1qtunnel
  dot1q pvc transport 201:any
   bind interface my_vpls_bridge local

 ! create PVC that matches double-tagged packet with outer tag 300
 dot1q pvc 300 encapsulation 1qtunnel
  dot1q pvc transport 300:any
   bind interface my_L2_bridge local
```

1.70 dot1q tunnel

dot1q tunnel ethertype ***tunl-type***

{**no** | **default**} **dot1q tunnel ethertype** ***tunl-type***

1.70.1 Purpose

Specifies the type of traffic (the type found in the 802.1Q header) for any 802.1Q tunnel configured on this port.

1.70.2 Command Mode

Port configuration

1.70.3 Syntax Description

ethertype ***tunl-type***	Type of 802.1Q traffic for this port, according to one of the following argument or keywords (in hexadecimal format): • ***user***—Custom traffic type; the range of values is 0x0 to 0xffff. • **8100**—Specifies the 8100 packet type; this is the default packet type. • **88a8**—Specifies the 88a8 packet type. • **9100**—Specifies the 9100 packet type. • **9200**—Specifies the 9200 packet type.

1.70.4 Default

The default packet type is 8100.

1.70.5 Usage Guidelines

Use the **dot1q tunnel** command to specify the type of traffic (the type found in the 802.1Q header) for any 802.1Q tunnel configured on this port.

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

1.70.6 Examples

The following example shows how to specify **9100** as the packet type:

```
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q tunnel ethertype 9100
```

1.71 download aaa route

download aaa route [**reset-interval**]

1.71.1 Purpose

Manually triggers an immediate route download.

1.71.2 Command Mode

exec

1.71.3 Syntax Description

reset-interval	Optional. Resets the route download timer.

1.71.4 Default

The value of the route download timer is maintained.

1.71.5 Usage Guidelines

Use the **download aaa route** command to manually trigger an immediate route download.

1.71.6 Examples

The following example shows how to manually trigger an immediate route download and reset the route download timer:

```
[local]Redback(config)# download aaa route reset-interval
```

1.72 drop (forward policy)

drop

no drop

1.72.1 Purpose

Drops incoming packets for this forward policy or this policy access control list (ACL) class.

1.72.2 Command Mode

- Forward policy configuration
- Policy group class configuration

1.72.3 Syntax Description

This command has no keywords or arguments.

1.72.4 Default

Packets are not dropped.

1.72.5 Usage Guidelines

Use the **drop** command to drop incoming packets according to the applied forward policy.

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

1.72.6 Examples

The following example shows how to configure the **DropPolicy** policy, which drops incoming packets that belong to the classes **ICMP** and **PIM:**

```
[local]Redback#config
[local]Redback(config)#forward policy DropPolicy
[local]Redback(config-policy-frwd)#access-group PBR_Drop_ACL local
[local]Redback(config-policy-group)#class ICMP
[local]Redback(config-policy-group-class)#drop
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class PIM
[local]Redback(config-policy-group-class)#drop
```

The following example shows how to configure the **DropAllPolicy** policy, which drops all incoming packets on the circuit:

```
[local]Redback#config
[local]Redback(config)#forward policy DropAllPolicy
[local]Redback(config-policy-frwd)#drop
```

1.73 drop (NAT policy)

drop

1.73.1 Purpose

Drops all packets or classes of packets associated with the Network Address Translation (NAT) policy.

1.73.2 Command Mode

- NAT policy configuration
- Policy group class configuration

1.73.3 Syntax Description

This command has no keywords or arguments.

1.73.4 Default

If no action is configured for the NAT policy, by default, packets are dropped.

1.73.5 Usage Guidelines

Use the **drop** command to drop all packets or classes of packets associated with the NAT policy.

1.73.6 Examples

The following example configures the **NAT-1** policy and applies the **NAT-ACL-1** access control list (ACL) to it. Packets that are classified as **NAT-CLASS-1** will be dropped. All other packets, except those explicitly defined by the static rule, will be ignored:

```
[local]Redback(config)#context CUSTOMER
[local]Redback(config-ctx)#nat policy NAT-1
[local]Redback(config-policy-nat)#ignore
[local]Redback(config-policy-nat)#ip static in source 10.0.0.1 171.71.71.1
[local]Redback(config-policy-nat)#access-group NAT-ACL-1
[local]Redback(config-policy-group)#class NAT-CLASS-1
[local]Redback(config-policy-group-class)#drop
```

1.74 drop source

drop source ***MAC-list-name***

no drop source ***MAC-list-name***

1.74.1 Purpose

Includes the specified MAC list filter criteria in the current bridge profile.

1.74.2 Command Mode

Bridge profile configuration

1.74.3 Syntax Description

MAC-list-name	Name of the list of MAC addresses.

1.74.4 Default

No default

1.74.5 Usage Guidelines

Use the **drop source** command to include the specified MAC list filter criteria in the current bridge profile.

See the **mac-list** command for instructions on setting up MAC list filters and for the detailed restrictions relevant to MAC list filters.

Use the **show circuit counters detail** command to show the number of dropped packets.

1.74.6 Examples

The following example illustrates how to create a MAC list named `noloops` with the **mac-list** command:

```
[local]Redback(config)#mac-list noloops
[local]Redback(config-mac-list)#11:11:11:ab:cd:cd
[local]Redback(config-mac-list)#11:13:44:ab:cd:ab
[local]Redback(config-mac-list)#end
```

The following example shows how to incorporate the created list in a bridge profile:

```
[local]Redback(config)#bridge profile mynetworkbridges
[local]Redback(config-bridge-profile)#drop source noloops
[local]Redback(config-bridge-profile)#end
```

The following example shows how to apply the bridge profile with the MAC list filter to a 802.1Q PVC that interfaces to a bridge where the filter is required:

```
[local]Redback(config)#port ethernet 5/2
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 5
[local]Redback(config-dot1q-pvc)#bridge profile mynetworkbridges
[local]Redback(config-bridge-profile)#end
```

1.75 dscp

dscp ***dscp***

no dscp ***dscp***

1.75.1 Purpose

Configures the DSCP value of the IP packet for a NAT logging profile.

For more information about how to configure NAT logging, see *nat logging-profile* and *Configure an Enhanced NAT Policy with Logging and Paired Mode*.

1.75.2 Command Mode

NAT logging configuration.

1.75.3 Syntax Description

dscp *dscp*	Optional. Defines the dscp value of the log packet, it defaults to ef. ***dscp*** can have the following values: • 0..63 Differentiated services codepoint value • 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 • ef Expedited Forwarding

1.75.4 Default

ef

1.75.5 Example

This example shows you how to configure a NAT logging profile that uses the DSCP value of `df` (Default Forwarding).

```
[local]Redback#configuration
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat
[local]Redback(config-ctx)#nat ?
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
[local]Redback(config-ctx)#nat logging-profile nat-log-profile
[local]Redback(config-nat-profile)#dscp df
```

1.76 dscp (CES)

dscp ***dscp***

no dscp ***dscp***

1.76.1 Purpose

Configures the diffserver code for the CES.

1.76.2 Command Mode

L2VPN configuration.

1.76.3 Syntax Description

dscp ***code***	***dscp*** can have the following values: • 0..63 Differentiated services codepoint value • 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 • all Map all DSCP values to the same value. • 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 • ef Expedited Forwarding

1.76.4 Default

0

1.76.5 Example

This example shows you how to configure the diffserver code for the CES over UDP PW.

```
[local]Redback(config)#l2vpn profile name1
[local]Redback(config-l2vpn-xc-profile)#peer xxx.xxx.xxx.xxx
[local]Redback(config-l2vpn-xc-profile)#exp-bits 3
[local]Redback(config-l2vpn-xc-profile)#tunnel lsp name2
[local]Redback(config-l2vpn-xc-profile)#dscp af13
```

1.77 dsu bandwidth

dsu bandwidth ***subrate***

{**no** | **default**} **dsu bandwidth**

1.77.1 Purpose

Sets the subrate bandwidth for the data service unit (DSU) on a clear-channel DS-3 channel or port.

1.77.2 Command Mode

DS-3 configuration

1.77.3 Syntax Description

subrate	Subrate, in Kbps, of the DSU on a clear-channel DS-3 channel or port. The range of values for a clear-channel DS-3 channel or port is 300 to 44,210; the default value is 44,210.

1.77.4 Default

The default value is 44,210 Kbps for a clear-channel DS-3 channel or port.

1.77.5 Usage Guidelines

Use the **dsu bandwidth** command to set the subrate bandwidth for the DSU on a clear-channel DS-3 channel or port if the DSU specified by the **dsu mode** command (in DS-3 configuration mode) is digital-link or larscom. The CLI responds to the ***subrate*** argument with the closest acceptable bandwidth, based on the time slot size for the DSU that you specified for this DS-3 channel or port.

Note: This command is not supported if the DSU specified by the **dsu mode** command is Kentrox.

Use the **no** or **default** form of this command to set the bandwidth to the default.

1.77.6 Examples

The following example shows how to set the bandwidth for the DSU on DS-3 channel **1** on channelized OC-12 port **1:**

```
[local]Redback(config)#port ds3 3/1:1
[local]Redback(config-ds3)#dsu bandwidth 20000
```

1.78 dsu mode

dsu mode {**digital-link** | **kentrox** | **larscom**}

{**no** | **default**} **dsu mode**

1.78.1 Purpose

Specifies the data service unit (DSU) vendor for a clear-channel DS-3 channel or port.

1.78.2 Command Mode

DS-3 configuration

1.78.3 Syntax Description

digital-link	Specifies Digital-Link as the vendor of the DSU; this is the default DSU vendor.
kentrox	Specifies Kentrox as the vendor of the DSU.
larscom	Specifies Larscom as the vendor of the DSU.

1.78.4 Default

The default value is the Digital-Link DSU vendor.

1.78.5 Usage Guidelines

Use the **dsu mode** command to specify the vendor of the DSU on a clear-channel DS-3 channel or port.

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

1.78.6 Examples

The following example shows how to specify the Larscom vendor for the DSU on clear-channel DS-3 channel **1** on channelized OC-12 port **1** in slot **3:**

```
[local]Redback(config)#port ds3 3/1:1

[local]Redback(config-ds3)#dsu mode larscom
```

1.79 dsu scramble

dsu scramble

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

1.79.1 Purpose

Enables payload scrambling on a clear-channel DS-3 channel or port.

1.79.2 Command Mode

DS-3 configuration

1.79.3 Syntax Description

This command has no keywords or arguments.

1.79.4 Default

Payload scrambling is disabled on the channel or port.

1.79.5 Usage Guidelines

Use the **dsu scramble** command to enable payload scrambling on a clear-channel DS-3 channel or port. The type of scrambling is dependent on the vendor selected for the DSU for a DS-3 channel or port by the **dsu mode** command (in DS-3 configuration mode).

Note: This command is not supported if the DSU specified by the **dsu mode** command is Larscom.

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

1.79.6 Examples

The following example shows how to enable payload scrambling on clear-channel DS-3 channel **1** on channelized OC-12 port **1** in slot **3:**

```
[local]Redback(config)#port ds3 3/1:1

[local]Redback(config-ds3)#dsu scramble
```

1.80 duplex

duplex ***mode***

{**no** | **default**} **duplex**

1.80.1 Purpose

Specifies the duplex mode for the SmartEdge 100 native or Gigabit Ethernet (GE) copper-based port if auto-negotiation is disabled and the port speed is set to 10 or 100 Mbps.

1.80.2 Command Mode

Port configuration

1.80.3 Syntax Description

mode

Port duplex mode, according to one of the following keywords:

- **half**—Half-duplex mode
- **full**—Full-duplex mode

1.80.4 Default

The mode of the port is full duplex.

1.80.5 Usage Guidelines

Use the **duplex** command to specify the duplex mode for the SmartEdge 100 native or GE copper-based port if auto-negotiation is disabled and the port speed is set to 10 or 100 Mbps. This command is ignored if auto-negotiation is enabled or if the speed of the port is set to 1000 Mbps.

To specify the copper interface for this port, use the **medium-type** command (in port configuration mode). To specify the speed for this port, use the **speed** command (in port configuration mode).

This command does not apply to GE ports on any other SmartEdge router or to any Fast Ethernet (FE) port on any SmartEdge router. To set the mode of an FE port, use the **medium** command (in port configuration mode).

Use the **no** or **default** form of this command to set the port duplex mode to the default condition.

1.80.6 Examples

The following example shows how to set the mode of a SmartEdge 100 native port **1** to half-duplex:

```
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#duplex half
```

1.81 dvsr-profile

dvsr-profile ***prof-name***

no dvsr-profile ***prof-name***

1.81.1 Purpose

Creates a dynamically verified static routing (DVSR) profile and enters DVSR profile configuration mode.

1.81.2 Command Mode

Context configuration

1.81.3 Syntax Description

prof-name	DVSR profile name.

1.81.4 Default

No DVSR profile is configured.

1.81.5 Usage Guidelines

Use the **dvsr-profile** command to create a DVSR profile, and enter DVSR profile configuration mode. You can use the DVSR profile to set the desired values for the DVSR operation. If no DVSR parameters are set, the profile uses default values for the DVSR parameters. All DVSR routes must reference an existing DVSR profile.

1.81.6 Examples

The following example shows how to define a DVSR profile, **abc-webfarm**, with a time-to-live (TTL) of **3**, a verification interval of **25** seconds, a timeout multiplier of **4**, and a minimum success of **2:**

```
[local]Redback(config)#context foo
[local]Redback(config-ctx)#dvsr-profile abc-webfarm
[local]Redback(config-dvsr)#ttl 3
[local]Redback(config-dvsr)#verify-set 25 timeout-multiplier 4 min-success 2
```

1.82 dynamic-hostname

dynamic-hostname [**display** | **router-name**]

no dynamic-hostname

1.82.1 Purpose

Configures a hostname for an Intermediate System-to-Intermediate System (IS-IS) instance.

1.82.2 Command Mode

IS-IS router configuration

1.82.3 Syntax Description

display	Optional. Displays the dynamic hostname mapping when any form of the **show isis** command in exec mode is used.
router-name	Optional. Displays the dynamic hostname for this IS-IS instance.

1.82.4 Default

If this command is not enabled, the name specified through the **system hostname** command in global configuration mode is used.

1.82.5 Usage Guidelines

Use the **dynamic-hostname** command to configure a hostname for an IS-IS instance.

Use the optional **display** keyword to enable dynamic hostname mapping for all **show isis** commands in exec mode.

By default, the hostname of the IS-IS instance is the name specified through the **system hostname** command in global configuration mode. Use the optional **router-name** keyword to allow a different hostname to be advertised for the IS-IS instance. This feature is useful when there are multiple IS-IS instances in that each IS-IS instance can display a different hostname. For information on the **system hostname** command, see the *Command List*.

Use the **no** form of this command to revert to the system hostname or remove dynamic hostname mapping used with **show isis** commands.

1.82.6 Examples

The following example shows how to configure dynamic-hostname mapping for the **isis_2** IS-IS instance:

```
[local]Redback(config-ctx)#router isis isis_2
[local]Redback(config-isis)#dynamic-hostname display
```

1.83 dynamic-path

dynamic-path ***er-name***

no dynamic-path

1.83.1 Purpose

Directs the Constrained Shortest Path First (CSPF) algorithm to dynamically compute the set of links and nodes that must be traversed.

1.83.2 Command Mode

RSVP LSP configuration

1.83.3 Syntax Description

er-name	Explicit route name.

1.83.4 Default

No dynamic path is applied to the label-switched path (LSP).

1.83.5 Usage Guidelines

Use the **dynamic-path** command to direct the CSPF algorithm to dynamically compute the set of links and nodes that must be traversed. The dynamic path name is the explicit route (ERO) name that you define using the **explicit-route** command in RSVP router configuration mode. The dynamic path references the ERO, which is a set of next hops that can be strict or loose. When you specify the next hop as strict or loose and apply it to an LSP, CSPF includes this specification as a constraint in its computation.

Note: You first configure the explicit route before you configure the dynamic path. For information about configuring the explicit route, see the **explicit-route** command in the *Command List*.

Use the **no** form of this command to delete a dynamic path that the CSPF algorithm applies to the LSP.

1.83.6 Examples

The following example shows how to configure the dynamic path `ex-route02`:

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp)#lsp lsp1
[local]Redback(config-rsvp-lsp)#dynamic-path ex-route02
```

1.84 dynamic-tunnel-profile (home agent instance)

dynamic-tunnel-profile ***profile***

no dynamic-tunnel-profile ***profile***

1.84.1 Purpose

In Home Agent configuration mode, applies a dynamic tunnel profile to a home-agent (HA) instance.

In FA Peer configuration mode, applies a dynamic tunnel profile to a foreign-agent (FA) peer.

1.84.2 Command Mode

- Home Agent configuration
- FA Peer configuration

1.84.3 Syntax Description

profile	Name of dynamic tunnel profile.

1.84.4 Default

The following are the defaults for the dynamic tunnel profile:

- **clear-df**—Disabled.
- **gre mtu** ***mtu***—1468 bytes
- **hold-time** seconds—30 seconds
- **ipip mtu** ***mtu***—1480 bytes
- **time-out** seconds—3 seconds

1.84.5 Usage Guidelines

Use the **dynamic-tunnel-profile** command (in Home Agent configuration mode) to apply a dynamic tunnel profile to an HA instance.

Use the **dynamic-tunnel-profile** command (in FA Peer configuration mode) to apply a dynamic tunnel profile to a FA peer.

You first create a dynamic tunnel profile in Mobile IP configuration mode and configure its attributes in Dynamic Tunnel Profile configuration mode. You then apply the profile to the HA instance (in Home Agent configuration mode) and its FA peers (in FA Peer configuration mode). Configured static tunnels take precedence over dynamic tunnels. When the dynamic tunnel profile is not applied to an FA peer, the peer inherits the profile specified in HA configuration mode. If you delete a referenced dynamic tunnel profile, the references to this profile are also deleted for the HA instance and FA peers. When this happens, the HA instance and FA peers use the default dynamic tunnel profile values. For information about how to create a dynamic tunnel profile, see Section 1.85 on page 181.

Note: You must configure a last-resort interface in the same context to use a dynamic tunnel profile. For information about configuring last-resort interfaces, see *Configuring Contexts and Interfaces*.

Use the **no** form of this command to delete the dynamic tunneling profile.

1.84.6 Examples

The following example shows how to create a last-resort interface, two dynamic tunnel profiles (`prof1` and `prof2`), and then apply these profiles to a HA instance and FA peer:

```
!Create dynamic tunnel profile prof1.
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof1
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#hold-time 10
[local]Redback(config-mip-dyn-tun1-profile)#time-out 10
[local]Redback(config-mip-dyn-tun1-profile)#ipip mtu 1200
[local]Redback(config-mip-dyn-tun1-profile)#end



!Create dynamic tunnel profile prof2

[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof2
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#hold-time 120
[local]Redback(config-mip-dyn-tun1-profile)#time-out 8
[local]Redback(config-mip-dyn-tun1-profile)#ipip mtu 1000
[local]Redback(config-mip-dyn-tun1-profile)#end
!Create last resort interface.
[local]Redback(config-ctx)#interface loop loopback
[local]Redback(config-if)#ip address 2.2.2.2/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface mip2 multibind lastresort
[local]Redback(config-if)ip unnumbered loop
```

```
! Apply dynamic tunnel profile prof1 to HA instance.

[local]Redback(config)#context ha
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#home-agent
[local]Redback(config-mip-ha)#dynamic-tunnel-profile prof1
[local]Redback(config-fa)#tunnel-type gre
[local]Redback(config-fa)#authentication none
[local]Redback(config-fa)#local-address to_fa


! Apply dynamic tunnel profile prof2 to FA peer 1.1.1.2.

[local]Redback(config-mip-ha)#foreign-agent-peer 1.1.1.2
[local]Redback(config-mip-ha-fapeer)#dynamic-tunnel-profile prof2
[local]Redback(config-mip-fa-fapeer)#end


! The FA peer 3.1.1.2 inherits dynamic tunnel profile prof1 (which is specified in HA configuration mode)
because no dynamic profile is applied at the FA peer level.

[local]Redback(config-mip-fa)#foreign-agent-peer 3.1.1.2
```

1.85 dynamic-tunnel-profile (foreign agent instance)

dynamic-tunnel-profile *profile*

no dynamic-tunnel-profile *profile*

1.85.1 Purpose

In Mobile IP configuration mode, creates a dynamic tunnel profile and enters Dynamic Tunnel Profile configuration mode.

In Foreign Agent configuration mode, applies the dynamic tunnel profile to an FA instance.

In HA peer configuration mode, applies a dynamic tunnel profile to an HA peer.

1.85.2 Command Mode

- Mobile IP configuration
- Foreign Agent configuration
- HA peer configuration

1.85.3 Syntax Description

profile	Name of dynamic tunnel profile.

1.85.4 Default

The following are the defaults for the dynamic tunnel profile:

- **clear-df**—Disabled.
- **gre mtu** *mtu*—1468 bytes
- **hold-time** seconds—30 seconds
- **ipip mtu** *mtu*—1480 bytes
- **time-out** *seconds*—3 seconds

1.85.5 Usage Guidelines

Use the **dynamic-tunnel-profile** command in Mobile IP configuration mode to create a dynamic tunnel profile and enter Dynamic Tunnel Profile

configuration mode. Dynamic Tunnel mode allows you configure dynamic tunnel profile attributes.

Use the **dynamic-tunnel-profile** command in Foreign Agent Configuration mode to apply a dynamic tunnel profile to a foreign-agent instance.

Use the **dynamic-tunnel-profile** command HA peer configuration mode to apply a dynamic tunnel profile to a home-agent peers.

Configured static tunnels take precedence over dynamic tunnels. If a dynamic tunnel profile is not applied to an HA peer, the peer inherits the dynamic tunnel profile specified in the FA instance. If there is no profile configured in this mode, the HA peer inherits the default dynamic tunnel profile values. If you delete a referenced dynamic tunnel profile, the references to this profile are also deleted by the FA instance and HA peer. When these references are deleted, the FA instance and HA peers use the default dynamic tunnel profile values. For information about applying a dynamic tunnel profile to a HA instance or FA peer, see Section 1.84 on page 178.

Note: You must configure a last-resort interface in the same context (FA context or VPN context) to use a dynamic tunnel profile. The last-resort interface must borrow an IP address using an unnumbered interface. For information about configuring last resort interfaces, see *Configuring Contexts and Interfaces*.

Use the **no** form of this command to delete a dynamic tunnel profile.

1.85.6 Examples

The following example shows how to create a last resort interface and dynamic tunnel profile, `prof1`, in Dynamic tunnel configuration mode and then apply the profile to an FA instance:

```
! Create a dynamic tunnel profile mode.
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof1
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#hold-time 10
[local]Redback(config-mip-dyn-tun1-profile)#time-out 10
[local]Redback(config-mip-dyn-tun1-profile)#ipip mtu 1200
[local]Redback(config-mip-dyn-tun1-profile)#end

Apply the dynamic tunnel profile prof1 to the FA instance.

[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#dynamic-tunnel-profile prof1

! Create a last resort interface with an IP unnumbered interface.
[local]Redback(config-ctx)#interface loop loopback
[local]Redback(config-if)#ip address 2.2.2.2/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface mip2 multibind lastresort
[local]Redback(config-if)ip unnumbered loop
```

The following example shows how to create a last resort interface, two dynamic tunnel profiles, `prof1` and `prof2`, and then apply profile`prof1` to an FA instance and `prof2` to an HA peer `1.1.1.2` . HA peer `3.1.1.2` inherits the dynamic tunnel profile `prof1` specified in FA configuration mode because no dynamic tunnel profiles are applied in HA peer level:

```
! Create dynamic tunnel profile prof1.

[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof1
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#hold-time 10
[local]Redback(config-mip-dyn-tun1-profile)#time-out 10
[local]Redback(config-mip-dyn-tun1-profile)#ipip mtu 1200
[local]Redback(config-mip-dyn-tun1-profile)#end


!Create dynamic tunnel profile prof2.

[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#dynamic-tunnel-profile prof2
[local]Redback(config-mip-dyn-tun1-profile)#clear-df
[local]Redback(config-mip-dyn-tun1-profile)#hold-time 120
[local]Redback(config-mip-dyn-tun1-profile)#time-out 8
[local]Redback(config-mip-dyn-tun1-profile)#ipip mtu 1000
[local]Redback(config-mip-dyn-tun1-profile)#end


! Create a last resort interface.

[local]Redback(config-ctx)#interface loop loopback
[local]Redback(config-if)#ip address 2.2.2.2/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface mip2 multibind lastresort
[local]Redback(config-if)ip unnumbered loop


! Apply the dynamic tunnel profile to the FA instance.

[local]Redback(config)#context fa
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#dynamic-tunnel-profile prof1
[local]Redback(config-fa)#tunnel-type gre
[local]Redback(config-fa)#authentication none
[local]Redback(config-fa)#local-address to_fa


! Apply the dynamic tunnel profile to the HA peer 1.1.1.2.

[local]Redback(config-mip-fa)#home-agent-peer 1.1.1.2
[local]Redback(config-mip-fa-hapeer)#dynamic-tunnel-profile prof2
[local]Redback(config-mip-fa-hapeer)#end


! HA peer 3.1.1.2 inherits dynamic tunnel profile prof1 (used by the FA instance) since no dynamic
profile is configured in HA peer configuration mode.

[local]Redback(config-mip-ha)#home-agent-peer 3.1.1.2
```