Ethernet Interface Configuration Mode Commands

Command Modes

The Ethernet Interface Configuration Mode is used to create and manage Ethernet IP interface parameters within a specified context.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Important

Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

bfd

Configures Bidirectional Forwarding Detection (BFD) interface parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

```
[no] bfd { echo [echo-interval interval_num] | interval interval_num }
    min_rx milliseconds multiplier value
```

no

Disables the specified option on this interface.

echo

Enables BFD echo mode.

BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for the detection process, therefore the number of BFD control packets that are sent out between two BFD neighbors is reduced.

Since the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.

echo-interval *interval_num*

Specifies the transmit interval between BFD echo packets. The default interval is 150 ms. The range is from 0 to 999 ms. (VPC only)

interval *interval_num*

Specifies the transmit interval (in milliseconds) between BFD packets.

- *For releases prior to 17.0*, *interval_num* is an integer from 50 through 999. (Default 50)
- *For release 17.0 onwards*, *interval_num* is an integer from 50 through 10000. (Default 50)

min_rx *milliseconds*

Specifies the receive interval in milliseconds for control packets.

- *For releases prior to 17.0*, *milliseconds* is an integer from 50 through 999. (Default 50)
- *For release 17.0 onwards*, *milliseconds* is an integer from 50 through 10000. (Default 50)

multiplier *value*

Specifies the value used to compute the hold-down time as a number from 3 to 50.

Usage Guidelines

Specify BFD parameters including echo mode and the transmit interval between BFD packets.

Example

To apply enable echo mode on this interface, use the following command:

```
bfd echo
```

The following command sets BFD interval parameters:

```
bfd interval 3000 min_rx 300 multiplier 3
```

crypto-map

Applies the specified IPSec crypto-map to this interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
crypto-map map_name [ secondary-address sec_ip_addr ]
no crypto-map map_name
```

no

Deletes the application of the crypto map on this interface.

map_name

Specifies the name of the crypto map being applied as an alphanumeric string of 1 through 127 characters that is case sensitive.

secondary-address *sec_ip_addr*

Applies the crypto map to the secondary address for this interface. *sec_ip_addr* must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should **not** be applied to interfaces.

The crypto map must be configured in the same context as the interface.

Example

To apply the IPSec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```

description

Sets the descriptive text for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
description  text
no description
```

no

Clears the description for the interface.

text

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

Usage Guidelines

Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

Example

```
description sampleInterfaceDescriptiveText
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines Use this command to return to the parent configuration mode.

ip access-group

Specifies the name of the Access Control List (ACL) group to assign to the interface.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
[ no ] ip access-group group_name { in | out } priority
```

no

Removes the ACL group from this interface.

group_name

Specifies the name of an existing ACL group as an alphanumeric string of 1 through 47 characters.

Important Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

{ in | out }

Specifies whether the ACL group will apply to inbound or outbound traffic.

priority

If more than one ACL group is applied, *priority-value* specifies the priority in which they will be compared against the packet. If not specified, the priority is set to 0. *priority-value* must be an integer from 0 through 4294967295. If access groups in the list have the same priority, the last one entered is used first.

Usage Guidelines

Specify the name of the Access Control List (ACL) group to assign to the interface along with its directionality and priority.

Example

```
ip access-group acl-101 in 56
```

ip address

Specifies the primary and optional secondary IPv4 addresses and subnets for this interface.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
ip address ip_address { mask | /mask } [ secondary ip_address ] [ srp-activate ]
no ip address ip_address
```

no

Removes the IPv4 address from this interface.

***ip_address*{ mask | /*mask* }**

Configures the IPv4 address and mask for the interface. *ip_address* must be entered using IPv4 dotted-decimal notation. IPv4 dotted-decimal or CIDR notation is accepted for the mask.

Important

For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

secondary *ip_address*

Configures a secondary IPv4 address on the interface.

Important

You must configure the primary IPv4 address before you will be allowed to configure a secondary address.

srp-activate

Activates the IP address for Interchassis Session Recovery (ICSR). Enable this IPv4 address when the Service Redundancy Protocol (SRP) determines that this chassis is ACTIVE. Requires an ICSR license on the chassis to activate.

Usage Guidelines The following command specifies the primary IP address and subnets for this interface.

Example

The following example configures an IPv4 address for this interface:

```
ip address 192.154.3.5/24
```

ip igmp profile

Associates an Internet Group Management Protocol (IGMP) profile with this interface.

Product All

Privilege Security Administrator, Administrator

Syntax Description **`[ no ] ip igmp profile`** *`profile_name`*

no

Removes the IGMP profile from this interface.

profile_name

Specifies the name of an existing IGMP profile as an alphanumeric string of 1 through 63 characters.

If the name is not for an existing profile, you are prompted to create a new profile. You are then moved to the IGMP Profile Configuration mode.

Usage Guidelines Associates an Internet Group Management Protocol (IGMP) profile with this interface.

Example

```
ip igmp profile default
```

ip mtu

Configures the Maximum Transmission Unit (MTU) for this interface.

Product All

Privilege Security Administrator, Administrator

Syntax Description

ip mtu *mtu_size* **[mru** *mru_size* **]**

no

Removes the MTU value.

mtu_size

Specifies the MTU in bytes as an integer from 576 though 2048.

mru_size

Specifies the MRU in bytes as an integer from 576 though 2048.

Usage Guidelines

For MTU,

IP MTU is supported for a normal interface and point-to-point interface (OLC ports).

The maximum MTU size allowed with an OLC port is 1600.

The maximum MTU size allowed with an Ethernet port is 2048. The default MTU size is 1500.

The maximum sizes for ethernet MTUs are:

- **Untagged traffic** (non-VLAN) – **ip MPU** *mtu-size* + ethernet header (20 bytes)
- **VLAN traffic** – **ip MPU** *mtu-size* + ethernet header (20 bytes) + vlan header (4 bytes)

Example

The following command sets the MTU value to *2048*.

```
ip mtu 2048
```

Usage Guidelines for MRU:

1. MRU attribute is optional and when it is not configured, MRU is set to the same value as MTU.
2. MRU optional attribute is not visible to users on VPC-DI and VPC-SI platforms. This is only visible on ASR 5500.
3. On nonlegacy ASR 5500 variants such as CUPS or ICUPS, the following error is shown to you when you try to configure MRU on an interface.

   ```
   Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
   enabled!
   ```

Example

The following command sets the MTU value to *2048*.

```
ip mtu 2048
```

The following command sets the MTU value to *1600* and MRU value to *1900*.

```
ip mtu 2048 mru 1900
```

ip ospf authentication-key

Configures the password for authentication with neighboring Open Shortest Path First (OSPF) routers.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

no

Deletes the authentication key.

encrypted

Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.

password *auth_key*

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

Usage Guidelines

Use this command to set the authentication key used when authenticating with neighboring routers.

Example

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

ip ospf authentication-type

Configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

no

Disable this function.

message-digest

Uses the message digest (MD) authentication method.

null

Uses no authentication, thus disabling either MD or clear text methods.

text

Uses the clear text authentication method.

Usage Guidelines

Use this command to set the type of authentication to use when authenticating with neighboring routers.

Example

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

ip ospf bfd

Enables or disables OSPF Bidirectional Forwarding Detection (BFD) on this interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf bfd [ disable ]
no ip ospf cost
```

no

Disable this function.

disable

Disables OSPF BFD on this interface.

Usage Guidelines

Enable or disable OSPF Bidirectional Forwarding Detection (BFD) on this interface.

Example

Use the following command to enable OSPF BFD;

```
ip ospf bfd
```

ip ospf cost

Configures the cost associated with sending a packet over the OSPF logical interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf cost value
no ip ospf cost
```

no

Disable this function.

value

Specifies the cost to assign to OSPF packets as an integer from 1 through 65535. Default: 10

Usage Guidelines

Use this command to set the cost associated with routes from the interface.

Example

Use the following command to set the cost to *20*;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

ip ospf dead-interval

Configures the interval that the router should wait, during which time no packets are received and after which the router considers a neighboring router to be off-line.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

`[ no ] ip ospf dead-interval` *`seconds`*

no

Returns the value to its default of 40 seconds.

seconds

Specifies the interval (in seconds) as an integer from 1 through 65535. This number is typical four times the hello-interval. Default: 40

Usage Guidelines

Use this command to set the dead intervals for OSPF communications.

Example

To set the dead-interval to *100*, use the following command;

```
ip ospf dead-interval 100
```

ip ospf hello-interval

Configures the interval (in seconds) between sending OSPF hello packets.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

`ip ospf hello-interval` *`seconds`*
`no ip ospf hello-interval`

no

Returns the value to its default of 10 seconds.

seconds

Specifies the number of seconds between sending hello packets as an integer from 1 through 65535. Default: 10

Usage Guidelines

Specify the interval (in seconds) between sending OSPF hello packets.

Example

To set the hello-interval to *25*, use the following command;

```
ip ospf hello-interval 25
```

ip ospf message-digest-key

Enables or disables the use of MD5-based OSPF authentication.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

ip ospf message-digest-key *key_id* **md5 [encrypted] password** *authentication_key*
no ip ospf message-digest-key *key_id*

no

Deletes the key.

message-digest-key *key_id*

Specifies the key identifier number as an integer from 1 through 255.

encrypted

Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

Usage Guidelines

Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example

To create a key with the ID of *25* and a password of *123abc*, use the following command;

```
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
no ip ospf message-digest-key 25
```

ip ospf network

Configures the Open Shortest path First (OSPF) network type.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |
point-to-point }
no ip ospf network
```

no

Disable this function.

broadcast

Sets the network type to broadcast.

non-broadcast

Sets the network type to non-broadcast multi access (NBMA).

point-to-multipoint

Sets the network type to point-to-multipoint.

point-to-point

Sets the network type to point-to-point.

Usage Guidelines

Use this command to specify the OSPF network type.

Example

To set the OSPF network type to *broadcast*, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

ip ospf priority

Designates the OSPF router priority.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf priority value
no ip ospf priority value
```

no

Disable this function.

value

Sets the priority value as an integer from 0 through 255.

Usage Guidelines

Use this command to set the OSPF router priority.

Example

To set the priority to *25*, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```

ip ospf retransmit-interval

Configures the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

no

Returns the value to its default of 5 seconds.

seconds

Specifies the number of seconds between LSA (Link State Advertisement) retransmissions as an integer from 1 through 65535. Default: 5

Usage Guidelines

Configure the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

Example

To set the retransmit-interval to *10*, use the following command;

```
ip ospf retransmit-interval 10
```

ip ospf transmit-delay

Configures the interval (in seconds) that the router should wait before transmitting an OSPF packet.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```

no

Returns the value to its default of 1 second.

seconds

Specifies the number of seconds that the router should wait before transmitting a packet as an integer from 1 through 65535. Default: 1

Usage Guidelines

Configure the interval (in seconds) that the router should wait before transmitting an OSPF packet.

Example

To set the transmit-delay to 5, use the following command;

```
ip ospf transmit-delay 5
```

ipv6 access-group

Specifies the name of the access control list (ACL) group to assign to this interface. You can filter for either inbound or outbound traffic.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

[no] ipv6 access-group *group name* **{ in | out } { priority-value** *priority_value* **}**

no

Removes a previously configured access group association.

group_name

Specifies the name of the access group as an alphanumeric string of 1 to 79 characters.

in

Applies the filter to the inbound traffic.

out

Applies the filter to the outbound traffic.

priority-value

Specifies the priority of the access group as an integer from 0 to 4294967295. 0 is the highest priority. If priority-value is not specified, the priority is set to 0.

If access groups in the list have the same priority, the last one entered is used first.

Usage Guidelines

Use this command to specify the ACL group to assign the interface to. Specify an ACL group name with this command.

Important

Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

Example

Use the following command to associate the *group_1* access group with the current IPv6 profile for inbound access:

```
ipv6 access-group group_1 in 1
```

ipv6 address

Specifies an IPv6 address and subnet mask.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

[no] ipv6 address *ipv6_address/mask*

no

Removes the IPv6 address from this interface.

ipv6_address/mask

Specifies an individual host IP address to add to this host pool in IPv6 colon-separated hexadecimal CIDR notation.

Important On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

Usage Guidelines

Configures the IPv6 address and subnet mask for a specific interface.

Example

The following example configures an IPv6 address for this interface:

```
ipv6 address 2002:0:0:0:0:0:c014:101/128
```

ipv6 ospf

Enables Open Shortest Path First Version 3 (OSPFv3) functionality on this IPv6 interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

[no] ipv6 ospf [area { *integer* | *ipv4-address* } | cost *cost-value* | dead-interval *dead-intrv* | hello-interval *hello-intrvl* | priority *p-value* | retransmit-interval *retx-interval* | transmit-delay *td-interval*]

no

Removes a previously configured access group association.

area { *integer* | *ipv4-address* }

Specifies an OSPFv3 area.

decimal_value: Specifies the identification number of the area as an integer from 0 through 4294967295.

ipv4-address: Specifies the IP address of the area in IPv4 dotted-decimal notation.

cost *cost-value*

Specifies a link cost as an integer from 1 through 65535. The link cost is carried in the LSA updates for each link. The cost is an arbitrary number.

dead-interval *dead-intrv*

Specifies the interval (in seconds) after which a neighbor is declared dead when no hello packets as an integer from 1 through 65535.

hello-interval *hello-intrvl*

Specifies the interval (in seconds) between hello packets that OSPFv3 sends on an interface as an integer from 1 through 65535.

priority *p-value*

Specifies the priority of the interface as an integer from 0 through 255.

retransmit-interval *retx-interval*

Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 interface as an integer from 1 through 65535.

transmit-delay *td-interval*

Specifies the estimated time (in seconds) required to send a link-state update packet on the interface as an integer from 1 through 65535.

Usage Guidelines

Configure an OSPFv3 interface in this context.

Example

```
ipv6 ospf area 334 cost 555 dead-interval 40 hello-interval 10 priority
10 retransmit-interval 5 transmit-delay 10
```

ipv6 router advertisement

Enables or disables the system to send IPv6 router advertisements.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

`[ no ] ipv6 router advertisement`

Usage Guidelines

Enables sending of router advertisements on the interface. All of the pool prefixes in the context (belonging to the interface) will be advertised in the router advertisement.

The router-lifetime in the advertisement is sent as 0 to indicate to the receiver that the sender cannot be a default-router. For all the prefixes (pools), the valid and preferred lifetime are sent as default. The router-advertisement is sent every 600 seconds.

If the pool-prefix is deleted, then router-advertisement is sent for that particular prefix with the valid and preferred time set to 0.

logical-port-statistics

Enables or disables the collection of logical port (VLAN and NPU) bulk statistics for the first 32 configured Ethernet or PVC interface types.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

`[ no ] logical-por t-statistics`

no

Stops the collection of logical port statistics on this interface.

Usage Guidelines

Starts or stops the collection of logical port bulkstats. Default: This feature is not enabled.

Statistics are collected for up to 32 logical ports. The system collects statistics on a per minute basis and maintains samples for the last 5-minute and 15-minute intervals when this feature is enabled.

Example

To start collection of logical port statistics on this interface, enter the following command:

```
logical-port-statistics
```

mpls ip

Enables or disables dynamic Multiprotocol Label Switching (MPLS) distribution and forwarding of IP packets on this interface.

Product

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

```
[ no ] mpls ip
```

no

Stops dynamic label distribution and forwarding on this interface.

Usage Guidelines

Starts label distribution and forwarding over an interface for a context that has MPLS enabled. For additional information, refer to the *Context Configuration Mode Commands* chapter. Default: This feature is not enabled.

Example

To start dynamic MPLS distribution and forwarding on this interface, enter the following command:

```
mpls ip
```

policy-forward

This command supports downlink IPv4 data packets received from the SGi that are forwarded/redirected to a configured next-hop address if the subscriber session does not exist in the P-GW.

Product

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

policy-forward { icmp unreachable next-hop *ip_address* **| unconnected-address next-system** *ip_address* **}**
no policy-forward unconnected-address

no

Deletes the policy forwarding configuration for unconnected address for the current interface.

icmp unreachable next-hop *ip_address*

Specifies routing of Internet Control Message Protocol (ICMP) unreachable is required in overlapping pool configuration. *ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

unconnected-address next-system *ip_address*

Specifies the IP address of the next system P-GW to handle processing during P-GW upgrade. *ip_address* must be an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Important The **unconnected-address next-system** *ip_address* keyword enables IPv4 downlink data packet forwarding/redirection.

Usage Guidelines

Use this command to set the redirecting policy for IP packets from an existing P-GW to a new P-GW during upgrade. To configure this command both keywords will be in separate interface.

Important This is a customer specific command.

Example

To configure existing P-GW system for redirecting the P-GW packets to new P-GW during existing P-GW upgrade enter the following commands:

```
policy-forward unconnected-address next-system ip_address
policy-forward icmp unreachable next-hop ip_address
```

pool-share-protocol

Configures the primary or secondary system for the IP pool sharing protocol and enter IPSP configuration mode.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

```
pool-share-protocol { primary ip_address | secondary ip_address } [ mode {
active | inactive | check-config } ]
no pool-share-protocol
```

no

Deletes the IP pool sharing protocol information from the current interface.

primary *address*

On the secondary system, defines the IP address of an interface on the primary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip_address* must be expressed in IP v4 dotted-decimal notation.

secondary *ip_address*

On the primary system, define the IP address of an interface on the secondary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip_address* must be expressed in IP v4 dotted-decimal notation.

mode { active | inactive | check-config }

This is an optional command to manage the mode for IP pool sharing protocol for primary or secondary HA.

active: Activates the IP pool sharing protocol mode.

inactive: Inactivates the IP pool sharing protocol mode.

check-config: Verifies the IP pool sharing protocol configuration.

Usage Guidelines

Use this command to set the IP address of the primary or secondary system for use with the IP pool sharing protocol and enter ipsp configuration mode. This command must be configured for an interface in each context that has IP pools configured. Refer to the *System Administration Guide* for information on configuring and using the IP pool sharing protocol.

Important Both the primary and secondary systems must be in the same subnet.

Important For information on configuring and using IP Pool Sharing Protocol (IPSP), refer to the *PDSN Administration Guide*.

Important Reserve free addresses on the primary HA for this command via the **reserved-free-percentage** command as described in the *IPSP Configuration Mode Commands* chapter of this guide.

Example

To configure a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10
```

To inactivate a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10 mode inactive
```

port-switch-on-L3-fail

Causes the ASR 5500 MIO port to which the current interface is bound to switch over to the port on the redundant line card or MIO when connectivity to the specified IP address is lost.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

```
port-switch-on-L3-fail address { ip_address | ipv6_address } [
minimum-switchover-period switch_time ] [ interval int_time ] [ timeout time_out
 ] [ num-retry number ]
no port-switch-on-L3-fail
```

no

Disable port switchover on failure.

ip_address

The IP address to monitor for connectivity, entered in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation.

minimum-switchover-period *switch_time*

After a switchover occurs, another switchover cannot occur until the specified amount of time (in seconds) has elapsed. The *switch_time* must be an integer from 1 through 3600. Default: 120

interval *int_time*

Specifies how often (in seconds) monitoring packets are sent to the IP address being monitored. The *int_time* must be an integer from 1 through 3600. Default: 60

timeout *time_out*

Specifies how long to wait (in seconds) without a reply before resending monitoring packets to the IP address being monitored. The *time_out* must be an integer from 1 through 10. Default: 3

num-retry *number*

Specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover. The *number* must be an integer from 1 through 100. Default: 5

Usage Guidelines

Use this command to monitor a destination in your network to test for L3 connectivity. The destination being monitored should be reachable from both the active and standby line cards.

Example

The following command enables port switchover on connectivity failure to the IP address *192.168.10.100* using default values:

```
port-switch-on-L3-fail address 192.168.10.100
```

The following command disables port switchover on connectivity failure:

```
no port-switch-on-L3-fail
```

vlan-map

Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The vlan-map is associated with a specific interface (ASR 5000 only).

Product

PDSN

HA

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-eth)#`

Syntax Description

`vlan-map next-hop` *`ip_address`*

next-hop *ip_address*

Specifies the IP address for the next-hop gateway in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to combine multiple VLAN links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.

After configuring the vlan-map, move to the Ethernet Port Configuration mode to attach the vlan-map to a specific VLAN.

Example

The following command sets an IPv4 address for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```