Context Configuration Mode Commands I-M

Command Modes

This section includes the commands **ikev1 disable-initial-contact** through **multicast-proxy** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

ikev1 disable-initial-contact

Disables the sending of the INITIAL-CONTACT message in the IKEv1 protocol after the node creates a new Phase1 SA, caused either by Dead Peer Detection or by a rekey.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

`[ no ] ikev1 disable-initial-contact`

no

Disables this command, which re-enables the sending of the INITIAL-CONTACT message.

Usage Guidelines

Use this command to disable the sending of the INITIAL-CONTACT message in the IKE v1protocol.

Example

The following command disables the sending of the INITIAL-CONTACT message:

`ikev1 disable-initial-contact`

ikev1 disable-phase1-rekey

Configures the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

`[ no ] ikev1 disable-phase1-rekey`

no

Re-enables Phase 1SAs when the ISAKMP lifetime expires.

Usage Guidelines

Use this command to disable the rekeying of Phase 1 SAs when the ISAKMP lifetime expires in IKE v1 protocol.

Example

The following command disables rekeying of Phase1 SAs when the lifetime expires:

`ikev1 disable-phase1-rekey`

ikev1 keepalive dpd

Configures the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] ikev1 keepalive dpd interval *interval* **timeout** *time* **num-retry** *retries*

no

Deletes previously configured IPSec DPD Protocol settings.

dpd interval *interval*

Specifies the time interval (in seconds) at which IPSec DPD Protocol messages are sent. *interval* is an integer from 10 through 3600.

timeout *time*

Specifies the amount of time (in seconds) allowed for receiving a response from the peer security gateway prior to re-sending the message. *time* is an integer from 10 through 3600.

num-retry *retries*

Specifies the maximum number of times that the system should attempt to reach the peer security gateway prior to considering it unreachable. *retries* is an integer from 1 through 100.

Usage Guidelines

Use this command to configure the ISAKMP dead peer detection parameters in IKE v1 protocol.

Tunnels belonging to crypto groups are perpetually kept "up" through the use of the IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

Important The peer security gateway must support RFC 3706 in order for this functionality to function properly.

This functionality is for use with the Redundant IPSec Tunnel Fail-over feature and to prevent IPSec tunnel state mismatches between the FA and HA when used in conjunction with Mobile IP applications.

Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the **show crypto isakmp security associations summary dpd** command.

Important If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

Example

The following command configures IPSec DPD Protocol parameters to have an interval of *15*, a timeout of *10*, to retry each attempt *5* times:

```
ikev1 keepalive dpd interval 15 timeout 10 num-retry 5
```

ikev1 policy

Configures or creates an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

`[ no ] ikev1 policy` *priority*

no

Removes a previously configured ISAKMP policy for IKE v1 protocol.

priority

Specifies the priority of an ISAKMP policy as an integer from 0 through 100. ISAKMP policies for IKE v1 protocol with lower priority numbers take precedence over policies with higher priorities. "0" is the highest priority. Default: 0

Usage Guidelines

Use this command to create ISAKMP policies to regulate how IPSec key negotiation is performed for IKE v1 protocol.

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKESAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

Multiple ISAKMP policies can be configured in the same context and are used in an order determined by their priority number.

Example

Use the following command to create an ISAKMP policy with the priority *1* and enter the ISAKMP Configuration Mode:

```
ikev1 policy 1
```

ikev2-ikesa

Creates a new, or specifies an existing, IKEv2 security association parameters and enters the IKEv2 Security Association Configuration Mode.

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

HeNBGW

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] ikev2-ikesa { auth-method-set *auth_method_set_name* **| certificate policy** *policy_name* **| ddos { blacklist ip-address** *ipv4_address | ipv6_address* **| [init-flood | udp-error] { source-based | system-based } [threshold-upper** *threshold_upper_value* **[threshold-lower** *threshold_lower_value* **[poll-timer-duration** *poll_timer_duration_value* **]]] } | dh-group { [1 | 14 | 2 | 5] + { | reuse } } | transform-set** *transform_set_name* **}**

{ default | no } ikev2-ikesa dh-group reuse

default

Sets the IKEv2 IKESA Diffie-Hellman related parameter to its default value.

Default: 14

no

Removes the entered IKEv2 security association parameters.

auth-method-set *auth_method_set_name*

Configure an IKEv2 IKE Security Association Auth-Method Set. Applicable for IKEv2 subscriber-mode based products, This object encapsulates various Authentication methods.

auth_method_set_name is the context level name to be used for the IKEv2 IKE Security Association Authentication methods Set, which is a string of size 1 to 127.

certificate policy *policy_name*

certificate: Configures certificate related configuration to be associated to crypto template.

policy: Configures certificate policy to be used for certificate related auth method.

policy_name is the context level name to be used for the IKEv2 Security Association Cert Policy, which is a string of size 1 to 127.

ddos

Configures the IKEv2 DDoS mitigation Parameters.

blacklist ip-address*ipv4_address* | *ipv6_address*

Configures the source IPv4 or IPv6 address to be blacklisted.

init-flood

Configures the IKEv2 DDoS mitigation parameters for INIT Floods.

udp-error

Configures the IKEv2 DDoS mitigation parameters for UDP errors.

dh-group

Configures the IKEv2 IKESA Diffie-Hellman related parameters.

1

Configures the Diffie-Hellman Group 1, 768-bit MODP Group.

14

Configures the Diffie-Hellman 14, 2048-bit MODP Group.

2

Configures the Diffie-Hellman 2, 1024-bit MODP Group.

5

Configures the Diffie-Hellman 5, 1546-bit MODP Group.

reuse

Configures the reuse responders key-pair for DH group(s).

+

Indicates that more than one of the previous keywords can be entered within a single command.

source-based threshold-upper *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at source IP address level.

threshold-upper *threshold_upper_value*: Configures upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

threshold-lower *threshold_lower_value*: Configures lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS INIT Floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

system-based threshold-upper *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at system level.

threshold-upper *threshold_upper_value*: Configures the upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

poll-timer-duration *poll_timer_duration_value*: Configures the IKEv2 DDoS INIT floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

transform-set *transform_set_name*

Configure an IKEv2 IKE Security Association Transform Set. This object encapsulates various IKEv2 IKE algorithm configurations which are required for establishing and IKEv2 IKE Security Assocation with a remote peer.

transform_set_name is the context level name to be used for the IKEv2 IKE Security Association Transform Set, which is a string of size 1 to 127.

Usage Guidelines

Use this command to create a new or enter an existing IKEv2 security association parameters set. A list of up to four separate transform-sets and three separate authentication method sets can be created.

Entering the command **transform-set** *transform_set_name* results in the following prompt:

```
[context_name]hostname(cfg-ctx-ikev2ikesa-tran-set)#
```

IKEv2 Security Association Configuration Mode commands are defined in the *IKEv2 Security Association Configuration Mode Commands* chapter.

Example

The following command configures an IKEv2 security association transform set called *ikesa3* and enters the IKEv2 Security Association Configuration Mode:

```
ikev2-ikesa transform-set ikesa3
```

ims-auth-service

This command enables the creation, configuration or deletion of an IMS authorization service in the current context.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ims-auth-service *auth_svc_name* **[-noconfirm]**
{ no | default } ims-auth-service *auth_svc_name*

no

Deletes the specified IMS authorization service within the current context.

default

Restores default state of IMS authorization service, disabled for a specific context.

auth_svc_name

Specifies name of the IMS authorization service as a unique alphanumeric string of 1 through 63 characters.

In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.

Important Service names must be unique across all contexts within the system.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/configure/delete an IMS authorization service for Gx interface support in the current context.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsa-service)

IMS authorization Service Configuration commands are described in the *IMS Authorization Service Configuration Mode Commands* chapter.

Important Whenever a new ims-auth-serv is configured using an endpoint that is used by another ims-auth-serv, then the diabase callbacks are overwritten with values of the new IMSA service. This is a limitation on the system to register only one application per endpoint. So, multiple IMSA services registering with same endpoint may not work properly. If such scenario occurs, configure a different endpoint name for the IMSA service being used and then remove and re-configure the IMSA service used.

Example

The following command configures an IMS authorization service named *ims_interface1* within the current context:

```
ims-auth-service ims_interface1
```

ims-sh-service

Creates the specified IP Multimedia Subsystem (IMS) Sh service name to allow configuration of an Sh service.

Product

PDIF

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ims-sh-service *name*
no ims-sh-service *name*

no

Removes a previously configured IMS-Sh-service.

name

Specifies the name of the IMS-Sh-service to be configured as an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

The IMS-Sh-service is named in the pdif-service and/or cscf-service. Use this command to enter the IMS Sh Service Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-ims-sh-service)#

IMS Sh Service Configuration Mode commands are defined in the *IMS Sh Service Configuration Mode Commands* chapter in this guide.

Example

The following example creates or enters an IMS Sh service named *ims-1*:

```
ims-sh-service ims-1
```

inspector

Configures a context-level inspector account within the current context.

Product

All

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
inspector user_name [ encrypted ] [ nopassword ] password password [ ecs |
noecs ] [ expiry-date date_time ] [ li-administration ] [ noconsole ] [ noecs
 ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [
timeout-idle timeout_duration ] [ timeout-min-idle idle_minutes ][
exp-grace-interval days][ exp-warn-interval days][ no-exp-grace-interval ][
 no-exp-warn-interval ]
no inspector user_name
```

no

Removes a previously configured inspector account.

user_name

Specifies a name for the context-level inspector account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level inspector privileges within the current context. The encrypted keyword indicates the password specified uses encryption.

password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password

keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

[nopassword]

This option allows you to create an inspector without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an inspector password to gain access to the user account.

ecs | noecs

Default: **noecs**

ecs: Permits the specific user to access ACS-specific configuration commands.

noecs: Prevents the specific user to access ACS-specific configuration commands.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

noconsole

Disables user access to a Console line.

Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

timeout-absolute *abs_seconds*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) the context-level inspector may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level inspector may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time (in seconds) the context-level inspector may have a session active before the session is terminated. *timeout_duration* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time (in minutes) the context-level inspector may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0

Usage Guidelines

Create new context-level inspector or modify existing inspector's options, in particular, the timeout values.

Inspector users have minimal read-only privileges. Refer to the *Command Line Interface Overview* chapter for more information.

Important A maximum of 128 administrative users and/or subscribers may be locally configured per context.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
inspector trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following command creates a context-level inspector account named *user1*:

inspector user1 password secretPassword

The following command removes a context-level inspector account named *user1*:

no inspector user1

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

inspector *user_name* **password** *password* **[max-age** *days***][password-exp-grace-interval** *days***][password-exp-grace-interval** *days***]**

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:

4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

interface

Creates or deletes an interface or specifies an existing interface. By identifying an interface, the mode changes to configure this interface in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
interface name [ broadcast | loopback | point-to-point  | tunnel |
unnumbered ]
no interface name
```

no

Removes the specified interface.

name

Specifies the name of the interface to configure. If *name* does not refer to an existing interface, the new interface is created if resources allow. *name* is an alphanumeric string of 1 through 79 characters.

broadcast

Creates an Ethernet broadcast (IP) interface and enters the Ethernet Configuration Mode. Default: Enabled

Important Refer to the *Ethernet Interface Configuration Mode Command* chapter for more information.

loopback

Creates an internal IP address that is always UP, is not bound to any physical card/port, and can be reached by any interface configured in the current context. As a loopback interface uses all available physical ports, this type of interface is particularly useful for load-balancing. The interface must be configured for loopback when configuring Interchassis Session Recovery (ICSR). A total of 256 loopback interfaces can be configured. Default: Disabled

This loopback option is not used to setup a diagnostic test port so it should not be confused with the loopback option used in the various card/port configuration modes.

Important Refer to the *Loopback Interface Configuration Mode Command* chapter for more information.

point-to-point

Creates a permanent virtual connection (PVC) in the current context and enters the PVC Configuration Mode. Currently, this type of interface is only used with an optical (ATM) line card.

Important Refer to the *PVC Interface Configuration Mode Command* chapter for more information.

tunnel

Creates a tunnel interface to support the various tunnel interfaces. Currently only IPv6-over-IPv4 and GRE tunnel interfaces are supported.

Important Refer to the *Tunnel Interface Configuration Mode Commands* chapter for more information.

unnumbered

Creates an unnumbered IP interface within the context. An unnumbered interface enables IP processing without assigning an explicit IP address to the interface. In StarOS this type of interface supports an untagged BFD port. The only parameter for this type of interface is a text description.

Important Refer to the *Unnumbered Interface Configuration Mode Commands* chapter for more information.

Usage Guidelines Use this command to enter or create the interface configuration mode for an existing interface or for a newly defined interface. This command is also used to remove an existing interface when it longer is needed.

Important If no keyword is specified, broadcast is assumed and the interface is Ethernet by default.

For IPv6-over-IPv4 or GRE tunneling, you need to specify the interface type as **tunnel**.

Example

The following command enters the Ethernet Interface Configuration Mode creating the interface *sampleService*, if necessary:

```
interface sampleInterface
```

The following command removes *sampleService* as being a defined interface:

```
no interface sampleInterface
```

The following command enters the Tunnel Interface Configuration Mode creating the interface *GRE_tunnel1*, if necessary:

```
interface GRE_tunnel1 tunnel
```

ip access-group

Configures an access group with an Access Control List (ACL) for IP traffic for the current context. The Context-level ACL is applied only to outgoing packets.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip access-group name [ in | out ] [ priority_value ]
no ip access-group name [ in | out ]
```

no

Indicates the specified ACL rule is to be removed from the group.

name

Specifies the ACL rule to be added/removed from the group.

In Release 8.1 and later, *name* is an alphanumeric string of 1 through 47 characters.

In Release 8.0, *name* is an alphanumeric string of 1 through 79 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 256-rule limit for the context.

in | out

The **in** and **out** keywords are deprecated and are only present for backward compatibility. The Context-level ACL are applied only to outgoing packets.

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified, the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 0

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

Usage Guidelines Use this command to add IP access lists (refer to the **ip access-list** command) configured with in the same context to an ACL group.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following commands add *sampleGroup* to the context-level ACL with a priority of *0*:

```
ip access-group sampleGroup 0
```

ip access-list

Create, configure, or delete an IP Access List in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip access-list name
{ default | no } ip access-list name
```

default

Sets the context's default access control list to that specified by *name*.

no

Removes the specified access list.

name

Specifies the access list name.

name is an alphanumeric string of 1 through 47 characters.

If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.

If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

Usage Guidelines

Executing this command enters the ACL Configuration Mode in which rules and criteria are defined for the ACL.

Important A maximum of 256 rules (21.4 and higher releases) or 128 rules (releases prior to 21.4) can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less then 200.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following command creates an access list named *sampleList*, and enters the ACL Configuration Mode:

```
ip access-list sampleList
```

ip arp

Configures the allocation retention priority (ARP) options for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip arp ip_address mac_address [ vrf vrf_name ]
no ip arp ip_address mac_address
```

no

Removes the ARP configuration data for the specified IP address from the configuration.

ip_address

Specifies the IP address for which to configure the ARP options where *ip_address* is an IP address expressed in IPv4 dotted-decimal notation.

mac_address

Specifies the media-specific access control layer address for the IP address. *mac_address* must be specified as a an 6-byte hexadecimal number with each byte separated by a colon, for example., "AA:12:bb:34:f5:0E".

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.

vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in *Context Configuration Mode* via the **ip vrf** command.

Usage Guidelines

Manage the IP address mapping which is a logical/virtual identifier to the more lower layer addressing used for address resolution in ICMP messages.

For tunnel-based interface, network IP pool can have overlapping ip-addresses across Verve. To manage it adding a preconfigured VRF context is required to associate with an static ARP entry. By default, the ARP is added in the given context. If the VRF name is specified, then the ARP is added to the VRF ARP table.

Example

The following commands set the IP and MAC address for the current context then remove it from the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7
no ip arp 10.2.3.4
```

The following commands set the IP and MAC address for a VRF context *vrf1* in the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7 vrf vrf1
```

ip as-path access-list

Defines Border Gateway Protocol (BGP) Autonomous System (AS) Path access lists.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description **`[ no ] ip as-path access-list`** *`list_name`* **`[ { deny | permit } `** *`reg_expr`* **`]`**

no

Remove the specified regular expression from the AS path access list.

list_name

Specifies the name of an AS path list as an alphanumeric string of 1 through 79 characters.

{ deny | permit }

deny: Denies access to AS paths that match the regular expression.

permit: Allows access to AS paths that match the regular expression.

reg_expr

A regular expression to define the AS paths to match. *reg_expr* is an alphanumeric string of 1 through 254 characters.

Important The **?** (question mark) character is not supported in regular expressions for this command.

Usage Guidelines Use this command to define AS path access lists for the BGP router in the current context. The chassis supports a maximum of 64 access lists per context.

Example

The following command creates an AS access list named *ASlist1* and permits access to AS paths:

```
ip as-path access-list ASlist1 permit
```

ip community-list

Configures filtering via a BGP community list. To filter by a BGP community, you must then match the community in a route-map.

Product All products supporting BGP routing

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip community-list { named named_list | standard  identifier } { deny | permit
 } { internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ... }
{ internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ...}
{ internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ...}
no ip community-list { named named_list | standard  identifier } { deny |
permit } { internet | local-AS | no-advertise | no-export | value
AS-community_number  }
```

no

Entering **no ip community-list** with a permit/deny clause deletes the matching community-list entry. Entering **no ip community-list** without a permit/deny clause deletes all the entries belonging to a community-list.

named *named_list*

Specifies the name of a community list as an alphanumeric string of 1 through 79 characters.

standard *identifier*

Specifies the name of a community list as an integer from 1 through 99.

{ deny | permit }

Specifies whether this community will deny or permit access to a specified destination.

{ internet | local-AS | no-advertise | no-export | value *AS-community_number*

Specifies the destinations to deny or permit for the community.

- **internet** – Advertise this route to the internet community, and any router that belongs to it.
- **local-AS** – Use in confederation scenarios to prevent sending packets outside the local autonomous system (AS).
- **no-advertise** – Do not advertise this route to any BGP peer, internal or external.
- **no-export** – Do not advertise to external BGP (eBGP) peers. Keep this route within an AS.
- **value** *AS-community_number* – Specifies a community string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters).

You can enter multiple destinations and AS community numbers separated by spaces.

Usage Guidelines

Configures filtering via a BGP community list. To filter by a BGP community, you must then match the community in a route-map.

Multiple community-list entries can be attached to a community-list by adding multiple permit or deny clauses for various community strings. Up to 64 community-lists can be configured in a context.

The communities-list is a way to group destinations into communities and apply routing decisions based on the communities. This method simplifies the configuration of a BGP speaker that controls distribution of routing information.

A community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators define to which communities a destination belongs.

Example

The following command specifies that community list number 5 will permit access to AS destination 200:5.

```
ip community-list standard 5 permit value 200:5
```

ip dns-proxy source-address

Enables the proxy DNS functionality and identifies this context as the destination context for all redirected DNS requests.

Important This command must be entered in the destination context for the subscriber. If there are multiple destination contexts for different subscribers, the command must be entered in each context.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description **`[ no ] ip dns-proxy source-address`** *`ip_address`*

no

Removes the address in this context as a destination for redirected DNS packets.

ip_address

Specifies an interface in this context used for redirected DNS packets. *ip_address* must be entered using IPv4 dotted-decimal notation.

Usage Guidelines Use this command to identify the interface in this context where redirected DNS packets are sent to the home DNS. The system uses this address as the source address of the DNS packets when forwarding the intercepted

DNS request to the home DNS server. For a more detailed explanation of the proxy DNS intercept feature, see the **proxy-dns intercept-list** command.

Example

The following command identifies an interface with an address of *10.23.255.255* in a destination context where the system forwards all intercepted DNS requests:

```
ip dns-proxy source-address 10.23.255.255
```

ip domain-lookup

Enables or disables domain name lookup via domain name servers for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip domain-lookup
no ip domain-lookup
```

no

Disables domain name lookup.

Usage Guidelines

Domain name look up is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

Example

```
ip domain-lookup
no ip domain-lookup
```

ip domain-name

Configures or removes a logical domain name for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

[no] ip domain-name *name*

no

Indicates the logical domain name for the current context is to be removed.

name

Specifies the logical domain name to use for domain name server address resolution. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP domain name.

Usage Guidelines

Set a logical domain name if the context is to be accessed by logical domain name in addition to direct IP address.

Example

```
ip domain-name sampleName.org
```

ip extcommunity-list

Configures route target filtering via a BGP extended community list. To filter by a BGP extended community, you must then match the extended community in a route-map.

Product

All products supporting BGP routing

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

ip extcommunity-list { named *named_list* **| standard** *identifier* **} { deny | permit } rt** *rt_number rt_number rt_number ...*
no ip community-list { named *named_list* **| standard** *identifier* **} { deny | permit } rt** *rt_number*

no

Entering **no ip extcommunity-list** with a permit/deny clause deletes the matching extended community-list entry. Entering **no ip extcommunity-list** without a permit/deny clause deletes all the entries belonging to an extended community-list.

named *named_list*

Specifies the name of an extended community list as an alphanumeric string of 1 through 79 characters.

standard *identifier*

Specifies the name of an extended community list as an integer from 1 through 99.

{ deny | permit }

Specifies whether this community will deny or permit access to a specific route target.

rt *rt_number*

Specifies a Route Target as a string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters). You can enter multiple route targets separated by spaces.

Usage Guidelines

Configures filtering via a BGP extended community list. To filter by a BGP extended community, you must then match the community in a route-map.

A BGP extended community defines a route target. MPLS VPNs use a 64-bit Extended Community attribute called a Route Target (RT). An RT enables distribution of reachability information to the correct information table.

Multiple extended community-list entries can be attached to an extended community-list by adding multiple permit or deny clauses for various extended community strings. Up to 64 extended community-lists can be configured in a context.

Example

The following command specifies that extended community list number 78 will deny access to route target 200:5:

```
ip extcommunity-list standard 78 deny rt 200:20
```

ip forward

Configures an IP forwarding policy to forward outgoing pool packets whose flow lookup fails to the default-gateway.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[ no ] ip forward outbound unused-pool-dest-address default-gateway
```

no

Disables forwarding to the default gateway.

outbound unused-pool-dest-address default-gateway

Enables forwarding to the default gateway.

Usage Guidelines

Use this command to set an IP forwarding policy that forwards outgoing pool packets whose flow lookup fails to the default gateway. By default, the behavior is to either send an ICMP Unreachable message or to discard the packet depending on the configuration of the IP pool.

Pool packets coming from the line card or MIO card whose flow lookup fails are discarded or ICMP unreachable is sent irrespective of whether this command is configured or not.

Note While this CLI is available on the ASR 5500, its functionality is not supported. Therefore, if the CLI is configured, it does not affect or alter the IP forwarding behaviour.

Example

To enable this functionality, enter the following command:

```
ip forward outbound unused-pool-dest-address default-gateway
```

To disable this functionality, enter the following command:

```
no ip forward outbound unused-pool-dest-address default-gateway
```

ip guarantee

Enables and disables local switching of framed route packets.

Product

GGSN

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[no] ip guarantee framed-route local-switching
```

no

Disables local switching of framed route packets.

framed-route local-switching

Enables local switching of framed route packets. By default, this functionality is disabled.

Usage Guidelines Use this command to enable and disable local switching of framed route packets. This functionality will be applicable only when there are some NEMO/framed route sessions in a context.

Example

The following command enables local switching of framed route packets:

```
ip guarantee framed-route local-switching
```

ip identification packet-size-threshold

Configures the packet size above which system will assign unique IP header identification.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip identification packet-size-threshold size
default ip identification packet-size-threshold
```

default

Restores default value of 576 bytes to IP packet size for fragmentation threshold.

size

Specifies the size of IP packet in bytes above which system will assign unique IP header identification for system generated IP encapsulation headers (such as MIP data tunnel). *size* is an integer from 0 through 2000. Default: 576

Usage Guidelines This configuration is used to set the upper limit of the IP packet size. All packets above that size limit will be considered "fragmentable", and an unique non-zero identifier will be assigned.

Example

The following commands set the IP packet size to 1024 bytes as threshold. above this limit system will assign unique IP header identification for system generated IP encapsulation headers:

```
ip identification packet-size-threshold 1023
```

ip igmp profile

Configures an Internet Group Management Protocol (IGMP) profile and moves to the IGMP Profile Configuration mode.

Product

PDSN

GGSN

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

`[ no ] ip igmp profile` *`name`*

no

Removes the specified IGMP profile.

name

Specifies the name of an IGMP profile as an alphanumeric string of 1 through 63 characters. If this is not the name of an existing profile, you are prompted to create the new profile.

Usage Guidelines

Configure and existing IGMP profile or create a new one. When this command is executed you are moved to the IGMP Profile Configuration mode. For additional information, refer to the *IGMP Profile Configuration Mode Commands* chapter.

Example

```
ip igmp profile default
```

ip localhost

Configures or removes the static local host logical name to IP address mapping for the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description **`[ no ] ip localhost`** *`name ip_address`*

no

Specifies that the static mapping must be removed.

name

Specifies the logical host name (DNS) for the local machine on which the current context resides. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP host name.

ip_address

Specifies the IP address for the static mapping. *ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines Avoid excessive DNS lookups across the network by statically mapping the logical host name to the local host's context.

Example

```
ip localhost localHostName 10.2.3.4
no ip localhost localHostName 10.2.3.4
```

ip name-servers

Modifies the list of domain name servers the current context may use for logical host name resolution.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

```
ip name-servers ip_address secondary_ip_address[third_ip_address]
no ip name-servers ip_address
```

no

Indicates the name server specified is to be removed from the list of name servers for the current context.

ip_address

Specifies the IP address of a domain name server using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

secondary_ip_address

Specifies the IP address of a secondary domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

third_ip_address

Specifies the IP address of a third domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. (VPC only)

Usage Guidelines

Manage the list of name servers the current context may use in resolving logical host names.

Note When this CLI configuration is changed, the DNS client is reinitialized and the **cache ttl negative** value is reset to the default value if **no cache ttl negative** is configured for the DNS client in the context.. Therefore, check and reconfigure the **no cache ttl negative** CLI after the **ip name-servers** CLI configuration is changed on the node.

The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN Configuration Mode with **dns** and **ipv6 dns** commands, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with **dns** and **ipv6 dns** commands has the third preference.
4. DNS values configured at context level has the last preference.

Important The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example

```
ip name-servers 10.2.3.4
```

ip pool

Enables creation, configuration or deletion of IP address pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ip pool *pool_name* { *ip_address/subnet_mask* | *ip_address_mask_combo* | **range** *start_ip_address end_ip_address* } [**address-hold-timer** *address_hold_timer*] [**address-quarantine-timer** *seconds*] [**advertise-if-used**] [**alert-threshold** [**group-available** | **pool-free** | **pool-hold** | **pool-release** | **pool-used**] *low_thresh* [**clear** *high_thresh*]] [**explicit-route-advertise**] [**group-name** *group_name*] [**include-nw-bcast**] [**napt-users-per-ip-address** *users_per_ip* [**alert-threshold** { { **pool-free** | **pool-hold** | **pool-release** | **pool-used** } *low_thresh* [**clear** *high_thresh*] } +] [**max-chunks-per-user** *max_chunks_per_user* [**nat-binding-timer** *nat_binding_timer*] [**nat-pkt-drop-threshold** *high_thresh* [**clear** *low_thresh*]] [**nexthop-forwarding-address** *ip_address*] [**on-demand**] [**port-chunk-size** *port_chunk_size*] [**port-chunk-threshold** *port_chunk_threshold*] [**send-nat-binding-update**] +] [**nat** *priority*] [**nat-one-to-one** [**alert-threshold** { { **pool-free** | **pool-hold** | **pool-release** | **pool-used** } *low_thresh* [**clear** *high_thresh*] } +] [**nat-binding-timer** *nat_binding_timer*] [**nat-pkt-drop-threshold** *high_thresh* [**clear** *low_thresh*]] [**nexthop-forwarding-address** *ip_address*] [**on-demand**] [**send-nat-binding-update**] +] [**nat-realm users-per-nat-ip-address** *users* [**on-demand [address-hold-timer** *address_hold_timer*]]] [**nexthop-forwarding-address** *ip_address* [**overlap vlanid** *vlan_id*] [**respond-icmp-echo** *ip_address*]] [**nw-reachability server** *server_name*] [**policy allow-static-allocation**] [**framed-route-vrf-list** *vrf_list_name*] [**pool-route** *ip_address/ip_mask*] [**private** *priority*] [**public** *priority*] [**resource** *priority*] [**send-icmp-dest-unreachable**] **[skip-nat-subscriber-ip-check]** [**srp-activate**] [**subscriber-gw-address** *ip_address*] [**static**] [**suppress-switchover-arps**] [**tag** { **none** | **pdif-setup-addr** }] [**unicast-gratuitous-arp-address** *ip_address*] [**vrf** *vrf_name* { [**mpls-label input** *in_label_value* | **output** *out_label_value1* [*out_label_value2*] }] [**framed-route-vrflist**] +

no ip pool *pool_name* **[address-hold-timer] [address-quarantine-timer] [advertise-if-used] [alert-threshold [[group-available] [pool-free] [pool-hold] [pool-release] [pool-used] +] [explicit-route-advertise] [group-name] [include-nw-bcast] [nexthop-forwarding-address [respond-icmp-echo]] [nw-reachability server] [policy allow-static-allocation] [framed-route-vrf-list] [send-icmp-dest-unreachable] [skip-nat-subscriber-ip-check] [srp-activate] [subscriber-gw-address] [suppress-switchover-arps] [**

tag { none | pdif-setup-addr }] [unicast-gratuitous-arp-address] + [send-nat-binding-update] [framed-route-vrflist]

no

Removes the specified IP address pool from the current context's configuration, or disables the specified option(s) for the specified IP pool.

no alert-threshold

This command without any optional keywords disables all alert thresholds.

name

Specifies the logical name of the IP address pool. *name* must be an alphanumeric string of 1 through 31 characters.

Important An error message displays if the **ip** *pool name* and the *group name* in the configuration are the same. An error message displays if the **ip** *pool name* or *group name* are already used in the context.

ip_address

Specifies the beginning IP address of the IP address pool using IPv4 dotted-decimal.

subnet_mask

Specifies the IP address mask bits to determine the number of IP addresses in the pool. *ip_mask* must be specified using IPv4 dotted-decimal notation.

1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.

0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match – the bit can be either a 0 or a 1.

For example, if the IP address and mask are specified as *172.168.10.0* and *255.255.255.224*, respectively, the pool will contain IP addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. *ip_address_mask_combo* must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

range *start_ip_address end_ip_address*

Specifies the IP addresses for the IP pool as a range of addresses.

start_ip_address specifies the beginning of the range of addresses for the IP pool.

end_ip_address specifies the end of the range of addresses for the IP pool.

The IP address range must be specified using IPv4 dotted-decimal notation.

For example, if *start_ip_address* is specified as *172.168.10.0* and *end_ip_address* is specified as *172.168.10.31* the IP pool will contain addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

private [*priority*]

Address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

public [*priority*]

Address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

static

Designates local IP address pool to statically assign pooled addresses.

Important The keyword **static** must be used for DHCP served IP addresses.

tag { none | pdif-setup-addr }

Default: **none**

none: default tag for all IP address pools

pdif-setup-addr:pool with this tag should only be used for PDIF calls.

address-hold-timer *seconds*

When this is enabled, and an active subscriber is disconnected, the IP address is held or considered still in use, and is not returned to the free state until the address-hold-timer expires. This enables subscribers who reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool.

seconds is the time in seconds and must be an integer from 0 through 31556926.

Important *For releases prior to 20.0*, a change made to the IP pool hold timer takes immediate effect on existing addresses currently on hold. Timeouts are adjusted to align with the new value. *For releases after 20.0*, the new timeout value will only be applied to addresses which are put on hold in the future. Timeouts for addresses currently in the hold state are not modified. They will timeout using the original timeout value.

Important Currently, the address-hold-timer only supports IPv4 addresses.

address-quarantine-timer *seconds*

Specifies the timer value in seconds for an address quarantine timer as an integer from 20 through 86400. This timer cannot be configured with an address-hold-timer in the same pool.

The IP pool address-quarantine-timer is a mechanism to busy out a released IP address for a specified interval. This prevents an IP address from being reused until the quarantine timer expires.

Each IP pool can be configured with a timer value that determines how long a recently released address will be held in quarantine before being freed. When the timer has expired, the address is returned to the list of free addresses, to be allocated again to a new subscriber. Any address that has been released, but for which the address-quarantine-timer has not expired, is still considered to be in use for the purposes of allocation. If a subscriber tries to reconnect while the address-quarantine timer is armed, even though it is the same subscriber ID, the subscriber does not get the same address.

advertise-if-used

Advertises to the peer routes only if addresses are being used in pool.

alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*]

Default: All thresholds are disabled.

Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds.

group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group.

pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.

pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.

pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.

pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

Important Refer to the **threshold available-ip-pool-group** and **threshold monitoring** commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100.

clear *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. It may be configured as an integer between 0 and 100.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

group-name *group_name*

Assigns one or more preconfigured IP pools to the IP pool group. *group_name* is case sensitive and must be an alphanumeric string of 1 through 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool(s).

IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool's addresses are exhausted the pool with the next highest precedence is used.

include-nw-bcast

Allows pools to include the classful network and broadcast addresses that are usually excluded when a pool crosses the classful network boundaries.

To remove the **include-nw-bcast** option from the ip pool, use the **no ip pool test include-nw-bcast** command.

napt-users-per-ip-address *users_per_ip* [alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [max-chunks-per-user *max_chunks_per_user* [nat-binding-timer *nat_binding_timer*] [nat-pkt-drop-threshold *high_thresh* [clear *low_thresh*]] [nexthop-forwarding-address *ip_address*] [on-demand] [port-chunk-size *port_chunk_size* [min-port-chunk-per-user *chunks*]] [port-chunk-threshold *port_chunk_threshold*] [send-nat-binding-update] +

Important In UMTS deployments this keyword is available in 9.0 and later releases. In CDMA deployments this keyword is available in 8.3 and later releases.

Important In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures many-to-one NAT realms.

- *users_per_ip*: Specifies how many users can share a single NAT IP address.

  In 18 and earlier releases, *users_per_ip* must be an integer from 2 through 2016.

  In 19 and later releases: *users_per_ip* must be an integer from 2 through 8064.

- **alert-threshold**: Specifies the alert threshold for the pool:

Important Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in. Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in that context, and override the threshold configurations set within individual pools.

  - **pool-free**: Percentage free alert threshold for this pool
  - **pool-hold**: Percentage hold alert threshold for this pool

- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.

Important The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **max-chunks-per-user** *max_chunks_per_user*: Specifies the maximum number of port chunks to be allocated per subscriber in the many-to-one NAT pool.

  In 18 and earlier releases: *max_chunks_per_user* must be an integer from 1 through 2016.

  In 19 and later releases: *max_chunks_per_user* must be an integer from 1 through 8064.

  Default: 1
- **min-port-chunk-per-user***min_port-chunk_per_user*: Configures NAT Port minimum number of chunks per user for many-to-one NAT pool.

  In 21.23 and later releases: *max_chunks_per_user* must be an integer from 1 through 100.
- **nat-binding-timer** *binding_timer*: Specifies NAT Binding Timer for the NAT pool. *timer* must be an integer from 0 through 31556926. If set to 0, is disabled. Default: 0
- **nat-pkt-drop-threshold** *high_thresh* **[clear** *low_thresh* **]**: Specifies the NAT packet drop threshold in percentage (%).

  high_thresh specifies the high NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

  clear *low_thresh* specifies the low NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0
- **nexthop-forwarding-address** *address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

Important The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release 9.0 and in 10.0 and later releases.

Important

- The minimum port chunk per user is only applicable to NAPT single-ip.
- **min-port-chunk-per-user** and **port-chunk-threshold** are mutually exclusive.

- **on-demand**: Specifies allocating IP when matching data traffic begins.
- **port-chunk-size** *size*: Specifies NAT port chunk size (number of NAT ports per chunk) for many-to-one NAT pool.

  In 18 and earlier releases: *size* must be an integer from 32 through 32256 (in multiples of 32).

  In 19 and later releases: *size* must be an integer from 8 through 32256 (in multiples of 8).

Important The **port-chunk-size** configuration is only available for many-to-one NAT pools.

Important The **port-chunk-size** must be a minimum of *64* with systems configured as an A-BG or P-CSCF.

- **port-chunk-threshold** *chunk_threshold*: Specifies NAT port chunk threshold in percentage of number of chunks for many-to-one NAT pool. *chunk_threshold* must be an integer from 1 through 100. Default: 100%

Important The **port-chunk-threshold** configuration is only available for many-to-one NAT pools.

- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

Important **send-nat-binding-update** is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the many-to-one NAT pool configuration:

- **group-name** *group_name*: Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.

  This keyword is available for NAT pool configuration only in Release 10.0 and later.

  NAT pool and NAT pool group names must be unique.

  group_name is an alphanumeric string of 1 through 31 characters that is case sensitive.

- **srp-activate**

  Activates the IP pool for Interchassis Session Recovery (ICSR).

nat *priority*

Designates the IP address pool as a Network Address Translation (NAT) address pool.

priority specifies the priority of the NAT pool. 0 is the highest priority. If *priority* is not specified, the priority is set to 0.

Must be a value from 0 (default) to 10.

Important This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

nat-one-to-one [alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [nat-binding-timer *nat_binding_timer*] [nat-pkt-drop-threshold *high_thresh* [clear *low_thresh*]] [nexthop-forwarding-address *ip_address*] [on-demand] [send-nat-binding-update] +

Important In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

Important In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to Release 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures one-to-one NAT realm.

- **alert-threshold**: Specifies alert threshold for this pool:

Important Thresholds configured using the **alert-threshold** keyword are specific to the pool in which they are configured. Thresholds configured using the **thresholdip-pool *** commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.

- **pool-free**: Percentage free alert threshold for this pool
- **pool-hold**: Percentage hold alert threshold for this pool
- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.

Important The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **nat-binding-timer** *nat_binding_timer*: Specifies NAT Binding Timer for the NAT pool. *binding_timer* must be an integer from 0 through 31556926. If set to 0, is disabled.

Important For many-to-one NAT pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT pools, it is 0. By default, the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.

- **nat-pkt-drop-threshold** *high_thresh* **[clear** *low_thresh* **]**: Specifies the NAT packet drop threshold in percentage (%).

  high_thresh specifies the high NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

  clear *low_thresh* specifies the low NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

- **nexthop-forwarding-address** *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

Important The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release9.0 and in Release 10.0 and later releases.

- **on-demand**: Specifies allocating IP address when matching data traffic begins.
- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

Important **send-nat-binding-update** is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the one-to-one NAT pool configurations:

- **address-hold-timer** *address_hold_timer*
- **group-name** *group_name*: specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group. NAT pool and NAT pool group names must be unique. *group_name* is an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is available for NAT pool configuration only in StarOS 10.0 and later releases.
- **srp-activate**:Activates the IP pool for Interchassis Session Recovery (ICSR).

nat-realm users-per-nat-ip-address *users* [on-demand [address-hold-timer *address_hold_timer*]]

Important In UMTS deployments, the **nat-realm** keyword is only available in Release 8.1.

Important In Release 8.1, the NAT On-demand feature is not supported.

Important This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

Designates the IP address pool as a Network Address Translation (NAT) realm pool.

users-per-nat-ip-address *users*: specifies the number of users sharing a single NAT IP address as an integer from 1 through 5000.

on-demand: Specifies to allocate IP when matching data traffic begins.

address-hold-timer *address_hold_timer*: Specifies the address hold timer (in seconds) for this pool as an integer from 0 through 31556926. If set to 0, the address hold timer is disabled.

Important Currently, the address-hold-timer only supports IPv4 addresses.

nexthop-forwarding-address *ip_address*

A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address.

overlap vlan id *vlan_id*

When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN). *vlan_id* is the identification number of a VLAN assigned to a physical port and can be configured to any integer from 1 through 4095.

For more information on configuring VLANs, refer to the *System Administration Guide*.

Important This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN. This keyword can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IPPDSN. For GGSNs, the total number of pools is limited by the number of VLANs defined but the maximum number per context is 256. Additional network considerations and configuration outside of the system maybe required.

nw-reachability server *server_name*

Binds the name of a configured network reachability server to the IP pool and enables network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.

server_name: Specifies the name of a network reachable server that has been defined in the current context, expressed as an alphanumeric string of 1 through 16 characters.

Important Also see the following commands for more information: Refer to the **policy nw-reachability-fail** command in the HA Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the **nw-reachability server** command in this chapter to configure network reachability servers. Refer to the **nw-reachability-server** command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.

respond-icmp-echo *ip_address*

Pings the first IP address from overlapping IP address pools.

Important In order for this functionality to work, all of the pools should contain an initial IP address that can be pinged.

resource

Specifies this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that also exist in other resource pools. IP addresses from a resource pool should not be used for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs. Default: Disabled

Also refer to the *Subscriber Configuration Mode Commands* chapter for a description of the **l3-to-l2-tunnel address-policy** command.

send-icmp-dest-unreachable

When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool.

Default: Disabled

skip-nat-subscriber-ip-check

When enabled, this is configured to skip private IP address check for non-NAT pools. This can be configured only for non-NAT pools during call-setup if NAT is enabled for the subscriber. If NAT is disabled, this value is not considered.

Default: Disabled (subscriber IP check is done).

explicit-route-advertise

When enabled, the output of **show ip pool verbose** includes the total number of explicit host routes. Default: Enabled

srp-activate

Activates the IP pool for Interchassis Session Recovery (ICSR).

subscriber-gw-address*ip_address*

Configures the subscriber gateway address for this pool.

Important Using this keyword might give a message as "busyout configured". This indicates that one ip address is reserved as subscriber-gw-address and not the entire pool.

suppress-switchover-arp

Suppress corresponding gratuitous ARP generation when a line card or MIO card switchover occurs. Default: Disabled

unicast-gratuitous-arp-address *ip_address*

Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required. Default: Perform broadcast gratuitous ARP.

vrf *vrf_name* { [mpls-label input *in_label_value* | output *out_label_value1* [*out_label_value2*] }

Associates a preconfigured Virtual Routing and Forwarding (VRF) instance with this IP pool and configures MPLS label parameters.

Important This command must be used with next-hop parameters.

vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context Configuration Mode through **ip vrf** command.

- *in_label_value* is the MPLS label that identifies the inbound traffic destined for this pool.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to the outgoing packets sent for subscribers from this pool. Where *out_label_value1* is the inner output label and *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

By default, the pools configured are bound to the default VRF unless specified with a VRF name.

Important You cannot have overlapping pool addresses using the same VRF. Also you cannot have two pools using different VRFs but the same in-label irrespective of whether or not the pools overlap. The pool must be private or static in-order to be associated with a certain VRF. If the VRF with such a name is not configured, you are prompted to add the VRF before configuring a pool.

policy allow-static-allocation

Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

Important In static allocation scenario, the pool group name is returned by AAA in the attribute **SN1-IP-Pool-Name**, and the IP address to use will be returned in the **Framed-IP-Address** attribute.

framed-route-vrf-list*vrf_list_name*

Configures a vrf-list in order for NVSE VRF authorization.

pool-route ***ip_address/ip_mask***

Configures the IP pool route instead of generating by-default. The address followed by the **pool-route** keyword can be an IPv4 or IPv6 address with the mask value.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

Define one or more pools of IP addresses for the context to use in assigning IPs to mobile stations. This command is also useful in resizing existing IP pools to expand or contract the number of addresses allocated. If you resize an IP pool, the change is effective immediately.

When using the **ip pool** command to resize an IP pool, the type must be specified since by default the command assumes the type as public. In other words, the CLI syntax to resize an IP pool is the same syntax used to create the pool. See examples below.

```
ip pool pool1 100.1.1.0/24 static
```

The syntax to resize that pool would be:

```
ip pool pool1 100.1.1.0/25 static
```

A pool which is deleted will be marked as such. No new IP addresses will be assigned from a deleted pool. Once all assigned IP addresses from a deleted pool have been released, the pool, and all associated resources, are freed.

Important If an IP address pool is matched to a ISAKMP crypto map and is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Over-lapping IP Pools: The system supports the configuration of over-lapping IP address pools within a particular context. Over-lapping pools are configured using either the resource or overlap keywords.

The **resource** keyword allows over-lapping addresses tunneled to different VPN end points.

The **overlap** keyword allows over-lapping addresses each associated with a specific virtual LAN (VLAN) configured for an egress port. It uses the VLAN ID and the nexthop address to determine how to forward subscriber traffic with addresses from the pool thus resolving any conflicts with overlapping addresses.

Note that if an overlapping IP Pool is bound to an IPSec Tunnel (refer to the **match ip pool** command in the *Crypto Group Configuration Mode* chapter), that tunnel carries the traffic ignoring the nexthop configuration. Therefore, the IPSec Tunnel takes precedence over the nexthop configuration. (Thus, one can configure the overlapping IP Pool with fake VLAN ID and nexthop and still be able to bind it to an IPSec Tunnel for successful operation.

The **overlap** keyword allows over-lapping addresses each associated with a specific VLAN can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 128 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per system.

Important Overlapping IP address functionality is currently supported for use with systems configured as an HA for Mobile IP, or as a PDSN for Simple IP, or as a GGSN. For deployments in which subscriber traffic is tunneled from the FA to the HA using IP-in-IP, a separate HA service must be configured for each over-lapping pool.

IP Pool Address Assignment Method: IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

Important Note that setting different priorities on each individual pool in a group can cause addresses in some pools to be used more frequently.

Important In NAT IP pool configurations, the minimum number of public IP addresses that must be allocated to each NAT pool must be greater than or equal to the number of Session Managers (SessMgrs) available on the system. On the ASR 5000, it is >= 84 public IP addresses. This can be met by a range of 84 host addresses from a single Class C. The remaining space from the Class C can be used for other allocations.

Example

The following commands define a private IP address pool, a public IP address pool, and a static address pool, respectively.

```
ip pool samplePool1 1.2.3.0 255.255.255.0 private
ip pool samplePool2 1.3.0.0 255.255.0.0 public
ip pool samplePool3 1.4.5.0 255.255.255.0 static
```

The following command defines a private IP pool specified with a range of IP addresses. The pool has 101 addresses.

```
ip pool samplePool4 range 10.5.5.0 10.5.5.100 private
```

The following command sets the address hold timer on the pool to *60* minutes (*3600* seconds):

```
ip pool samplePool4 address-hold-timer 3600
```

The following command removes the IP address pool from the configuration:

```
no ip pool samplePool1
```

The following command creates a static IP pool:

```
ip pool pool1 100.1.1.0/24 static
```

The following command resizes the static IP pool created in the previous example:

```
ip pool pool1 100.1.1.0/25 static
```

ip prefix-list

Creates an IP prefix list for filtering routes.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ip prefix-list name *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**
no ip prefix-list *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq *seq_number*

Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

any

Matches any prefix.

***network_address*/*net_mask* [ge *ge_value*] [le *le_value*]**

Specifies the prefix to match.

network_address/*net_mask*: the IP address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv4dotted-decimal notation. When neither **ge** (greater than or equal to) or **le** (less than or equal to) are specified an exact match is assumed.

ge *ge_value*: Specifies the minimum prefix length to match as an integer from 0 through 32. If only the ge value is specified, the range is from the ge value to 32. The ge value must be greater than *net_mask* and less than the le value.

le *le_value*: Specifies the maximum prefix length to match as an integer from 0 through 32. If only the le value is specified, the range is from the *net_mask* to the le value. The le value must be less than or equal to 32.

The following equation describes the conditions that ge and le values must satisfy:

net_mask < *ge_value* < *le_value* <= **32**

Usage Guidelines Use this command to filter routes by their IP prefix.

Example

```
ip prefix-list name prelist10 seq 5 permit 192.168.100.0/8 ge 12 le 24
```

ip prefix-list sequence-number

Enables or disables the inclusion of IP prefix list sequence numbers in the configuration file. This option is enabled by default.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description **[no] ip prefix-list sequence-number**

no

Disables the listing of IP prefix list sequence numbers in the configuration file.

Usage Guidelines Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IP prefix list sequence numbers in the configuration file, enter the following command:

```
no ip prefix-list sequence-number
```

ip route

Adds or removes routing information from the current context's configuration.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] ip route { *ip_address*/*ip_mask* | *ip_address ip_mask* } { *gateway_ip_address* | next-hop *next_hop_ip_address* | point-to-point | tunnel } *egress_intrfc_name* [cost *cost*] [fall-over bfd multihop *mhsess_name*] [precedence *precedence*] [vrf *vrf_name* [cost *value*] [fall-over bfd multihop *mhsess_name*] [precedence *precedence*] +

[no] ip route static bfd *if_name remote-endpt_ipv4_address*

[no] ip route static multihop bfd *mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr*

[no] ip route kernel ip_address/ip_address_mask_combo *egress_intrfc_name* **cost** *number*

[no] ip route kernel ip_address/ip_address_mask_combo *egress_intrfc_name* **cost** *number* **blackhole**

no

Indicates the route specified by this options is to be removed from the configuration.

kernel

Allows static route in the kernel routing table options.

ip_address/ip_mask | ip_address/ip_mask

Specifies a destination IP address or group of addresses that will use this route.

ip_address/ip_mask: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *ip_mask/* is entered using CIDR notation; the mask bits are a numeric value which is the number of bits in the subnet mask.

ip_address/ip_mask: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address* must be specified using the standard IPv4 dotted decimal notation. *ip_mask* must be specified using the standard IPv4 dotted decimal notation as network mask for subnets.

The mask as specified by *ip_mask* or resulting from *ip_address*/*ip_mask* is used to determine the network for packet routing.

0's in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing.

1's in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

ip_address/ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. *ip_address_mask_combo* must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value, which is the number of bits in the subnet mask.

gateway_ip_address | next-hop *next_hop_ip_address* | point-to-point | tunnel

Specifies which device or network to use when forwarding packets.

gateway_ip_address: Specifies the IP address of the network gateway to which to forward packets. The address must be entered in IPv4 dotted-decimal notation (###.###.###.###).

next-hop *next_hop_ip_address*: Specifies the next-hop IP address to which packets are to be forwarded. The address must be entered in IPv4 dotted-decimal notation.

point-to-point: Specifies that the egress port is an ATM point-to-point interface.

tunnel: Sets the static route for this egress interface as tunnel type, such as IPv6-over-IPv4 or GRE.

egress_intrfc_name

Specifies the name of the egress (out-bound) interface name in the current context as an alphanumeric string of 1 through 79 characters. For a blackhole route, the default is “*”, that is, a wildcard interface.

cost *cost*

Specifies the relative cost of the route. *cost* must be an integer from 0 through 255 where 255 is the most expensive. Default: 0

cost *number*

Defines the number of hops to the next gateway. The cost must be an integer from 0 through 255 where 255 is the most expensive. The default is 0.

blackhole

Defines blackhole route to install in the kernel to block or drop packets.

fall-over bfd multihop *mhsess_name*

Enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure. Specify *mhsess_name* as an alphanumeric string of 1 through 19 characters.

precedence *precedence*

Specifies the selection order precedence for this routing information. *precedence* must be an integer from 1 through 254 where 1 is the highest precedence. Default: 1

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration.

vrf_name is the name of a preconfigured VRF context configured in *Context Configuration Mode* via the **ip vrf** command.

static bfd *if_name remote-endpt_ipv4_address*

Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the *BFD Configuration Mode Commands* chapter.

if_name: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.

remote_endpt_ipv4_address: Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal notation.

static multihop bfd *mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr*

Creates a static multihop BFD route with local and remote endpoints.

mhbfd_sess_name: Specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.

local_endpt_ipaddress: Specifies the local endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

remote_endpt_ipaddress: Specifies the remote endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to configure IP route parameters. precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route's being selected first by lower precedence then the cost is used if multiple route's are defined with the same precedence.

This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

Important A maximum of 1,200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Important SNMP traps are generated when BFD sessions go up and down (BFDSessUp and BFDSessDown).

Use the **ip route kernel ip_address/ip_address_mask_combo interface** *interface_name* **cost** *number* to add the special route to any of two packet processing interfaces (SF cards) defined in the context configuration. Use the **[no] ip route kernel ip_address/ip_address_mask_combo interface** *interface_name* **cost** *number* **blackhole** to block or drop packets going out of the node.

Example

The following command adds a route using the combined IP address and subnet mask form:

```
ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
```

The following configures route options for a route specified using the distinct IP address and subnet mask form:

```
ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following deletes the two routes configured above:

```
no ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
no ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 10.2.3.0/32 tunnel egressSample1 precedence 160 vrf vrf1
```

ip routing maximum-paths

Enables Equal Cost Multiple Path (ECMP) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context.

Product All products that support Cost Multiple Path (CMP)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip routing maximum-paths [ max_num ]
[ default | no ] ip routing maximum-paths
```

default

Resets the command to its default setting of 4.

no

Disables ECMP for the current context.

max_num

The maximum number of ECMP paths that can be submitted by a routing protocol. *max_num* must be an integer within the following ranges:

- For ASR5000: 1 through 10
- For ASR5500: 1 through 24
- For VPC-DI: 1 through 32 (*for Releases prior to 21.4*
- For VPC-DI: 1 through 64 (*for Release 21.4+*

Default: 4

Usage Guidelines

Use this command to enable ECMP for routing and set the maximum number of ECMP paths that can be submitted by a routing protocol.

Example

To enable ECMP and set the maximum number of paths that may be submitted by a routing protocol in the current context to *10*, enter the following command:

```
ip routing maximum-paths 10
```

To disable ECMP in the current context, enter the following command:

```
no ip routing maximum-paths
```

ip routing overlap-pool

Configures the routing behavior for overlap-pool addresses.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[ no | default ] ip routing overlap-pool
```

default

Resets the command to its default setting of disabled.

no

Disables the routing behavior for overlap-pool addresses for the current context.

Usage Guidelines

Use this command configuration to advertise overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. If the "iprouting overlap-pool" is configured, then the overlap-addresses are added as interface addresses and advertised.

ip rri

Configures Reverse Route Injection (RRI) egress clear port IPv4 parameters. (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ip rri { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]
no ip rri { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI egress parameters.

ip_address

Specified in IPv4 dotted-decimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure RRI regress clear port IPv4 parameters.

Example

```
ip rri 10.1.1.1 interface rri02
```

ip rri-route

Configures High Availability (HA) IPv4 routing parameters for Reverse Route Injection (RRI). (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ip rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ip_address* } { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no ip rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ip_address* } { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI route.

network-mode { L2 | L3 }

Specifies the RRI route network mode type as Layer 2 (L2) or Layer 3 (L3).

clear_loopback_ip

Specifies the loopback address for clear traffic in IPv4 dotted-decimal notation.

rri-ip *virtual_ip_address*

Specifies the use of a virtual IP address on both Primary and Secondary for RRI. *virtual_ip_address* is expressed in IPv4 dotted-decimal notation.

ip_address

Specified in IPv4 dotted-decimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure HA IPv4 routing parameters for RRI.

Example

```
ip rri-route network-mode L3 rri-ip 10.1.1.23 next-hop 10.1.1.25 interface
 rriroute04
```

ip sri-route

Configures Layer 3 (L3) High Availability (HA) IPv4 routing parameters for Service Route Injection (SRI). (VPC-VSM only)

Product

Important The **ip sri-route** CLI command is deprecated, and not supported in 19.0 and later releases.

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ip sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**

no ip sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**

no

Disables the specified SRI route.

sri-ip *network_address*

Specifies the IPv4 address associated with the SRI route.

next hop *nexthop_address*

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through sixty-three characters.

Usage Guidelines

Use this command to configure L3 HA routing parameters for SRI.

Example

```
ip sri-route sri-ip 10.1.1.21 next-hop 10.1.1.23 interface sri23
```

ip vrf

Creates a Virtual Routing and Forwarding (VRF) context instance, assigns a VRF identifier, and configures the VRF parameters for BGP/MPLS VPN, GRE tunnel, and IPSec interface configuration.

Important IKEv2 ACL VRF is not supported.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
ip vrf vrf_name
no ip vrf
```

no

Disables IP Virtual Routing and Forwarding (VRF) parameters.

vrf_name

Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to create a VRF context and assign a VRF identifier for BGP/MPLS VPN, IPSec, GRE tunnel configuration in this context instance. This command is used when the system works as a BGP router with MPLS VPN and binds an MPLS VPN to the system or to facilitate GRE or IPSec tunnelling. The addresses assigned to this interface are visible in the VRF routing table.

This command switches the command mode to IP VRF Context Configuration Mode:

`[context_name>]host_name(config-context-vrf)#`

If required, this command creates an IP VRF Context Configuration Mode instance.

When using this command please note of the following:

- A VRF context instance must be created and configured before referring, associating, or binding the same with any command or mode.
- If the interface binding to a VRF context instance is changed or any IP address assigned to the interface is deleted, a warning is displayed.
- All interfaces bound with a VRF context instance will be deleted when that VRF is removed/deleted.
- An interface can be bound to only one VRF context instance.
- A maximum of 100 VRF context instances can be configured on a system.

Refer to the *IP VRF Context Configuration Mode Commands* chapter for parameter configuration.

Example

The following command configures the virtual routing and forwarding context instance *vrf1* in a context:

```
ip vrf vrf1
```

ip vrf-list

Creates a VRF list and adds VRFs to the list. The VRFs must have been previously created via the **ip vrf** command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

```
ip vrf-list list_name permit vrf_name
no ip vrf-list list_name [ permit vrf_name ]
```

no

Deletes a VRF list or delete VRFs from this list. If **permit** and *vrf-name* are not specified, the entire list of VRFs is deleted. Otherwise, the specified VRF(s) is deleted from the list.

list_name

Specifies the name of the VRF list as an alphanumerical string of 1 through 63 characters.

vrf_name

Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Create a VRF list and add VRFs to the list. The VRFs must have been previously created via the **ip vrf** command. This command supports multiple VRFs over NEMO.

Example

The following command creates a VRF list named *corp103* and adds a VRF named *vrf3567*:

```
ip vrf-list corp103 permit vrf3567
```

ipms

Enables/disables/manages an intelligent packet monitoring system (IPMS) client service and enters the IPMS Client Configuration Mode within the current context.

Product

IPMS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[ no ] ipms [ -noconfirm ]
```

no

Deletes a previously configured IPMS client service.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Caution If this keyword option is used with **no ipms** command, the IPMS client service will be deleted with all active/inactive IPMS sessions without prompting any warning or confirmation.

Usage Guidelines Use this command to enable/disable/manage the IPMS client service within a context and configure certain functionality. This command enables and allows the configuration of service enabling the system to function as an IPMS-enabled Access Gateway in a network. This command is also used to remove previously configured IPMS client service.

A maximum of 1 IPMS client can be configured per system.

Important The IPMS is a license enabled external application support. Refer to the *IPMS Installation and Administration Guide* for more information on this product.

Refer to the *IPMS Installation and Administration Guide* and *IPMS Configuration Mode* chapter of this reference for additional information.

Example

The following command creates an IPMS client service name within the context:

```
ipms
```

ipne-service

Create and/or configure an IPNE service.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config)#
```

Syntax Description

```
[ no ] ipne-service  ipne_service
```

no

Included as a prefix of the command, **no** causes the system to disable IPNE service when it has been created with this command and removes the IPNE service definition from the MME's configuration.

ipne_service

Enter 1 to 63 alphanumeric characters to create a unique name for an IPNE service instance.

Usage Guidelines

This command creates an instance of an IPNE service in the context.It is recommended that the IPNE Service be configured in the same context in which the MME Service has been configured.

This command also accesses the commands in the IPNE service configuration mode to configure the IPNE service.

If an IPNE service is to be removed and the service has active handles, then the handles are deleted using a timer-based approach and then the IPNE service is removed.

Example

Create an IPNE service called *IPNEserv1*:

```
ipne-service IPNEserv1
```

Use a command similar to the following to disable and remove the IPNE service configuration for the IPNE service called *ipneserv*.

```
no ipne-service ipneserv
```

ipsec replay

Configures IKEv2 IPSec specific anti-replay.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[ no ] ipsec replay [ window-size window_size ]
```

no

Disables this option.

replay

Configures IKEv2 IPSec anti-replay.

window-size *window_size*

Configures anti-replay window size.

window_size is the window size 32, 64 (default), 128, 256, 384, 512 , an integer value between 32..512

Usage Guidelines Use this command to configure IKEv2 IPSec specific anti-replay.

Example

The following command sets the window size to 256:

```
ipsec replay window-size 256
```

ipsec transform-set

Creates a new or specifies an existing IPSec transform set and enters the IPSec Transform Set Configuration Mode for the current context.

Product

ePDG

PDIF

SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
[ no ] ipsec transform-set transform_set_name
```

no

Removes an existing transform set from the system.

transform-set *name*

Specifies the name of a new or existing transform set as an alphanumeric string of 1 through 127 characters.

Usage Guidelines Use this command to Configure IKEv2 IPsec child security association transform set parameters. Up to four transform-sets can be created.

Entering this command results in the following prompt:

[*context_name*]*hostname*(cfg-ctx-ipsec-tran-set)#

This command applies to IKEv2. Please check **crypto ipsec transform-set** command for ipsec transform-set configuration for IKEv1.

Example

The following command configures an IPSec transform set called *ipsec12* and enters the IPSec Transform Set Configuration Mode:

ipsec transform-set *ipsec12*

ipsg-service

This command allows you to create/modify/delete an IP Services Gateway (IPSG) service in the current context.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipsg-service *ipsg_service_name* **[mode { radius-server [ewag] | radius-snoop }] [-noconfirm]**
no ipsg-service *ipsg_service_name* **[mode { radius-server [ewag] | radius-snoop }]**

no

If previously configured, deletes the specified IPSG service.

ipsg_service_name

Specifies the name of the IPSG service.

ipsg_service_name must be an alphanumeric string of 1 through 63 characters.

Important

Service names must be unique across all contexts within a chassis.

mode { radius-server [ewag] | radius-snoop }

Configures the IPSG to perform as either a RADIUS server or as a device to extract user information from RADIUS accounting request messages (snoop). If the optional keyword **mode** is not entered, the system defaults to **radius-server**.

- **radius-server**:Creates the named IPSG RADIUS Server service in the current context and/or enters the IPSG RADIUS Server Configuration Mode.
- **radius-server ewag**: Enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services.
- **radius-snoop**:Creates the named IPSG RADIUS Snoop service in the current context and/or enters the IPSG RADIUS Snoop Configuration Mode.

-noconfirm

Specifies to execute the command without additional prompt or confirmation.

Usage Guidelines

Use this command to create/configure/delete an IPSG service.

A maximum of one IPSG service can be configured per context.

IPSG service commands are defined in the *IPSG RADIUS Snoop Configuration Mode Commands* chapter and the *IPSG RADIUS Server Configuration Mode Commands* chapters.

A maximum of 256 services (regardless of type) can be configured per system.

Caution A large number of services greatly increases the complexity of system management and may impact overall system performance (i.e., resulting from system handoffs). Do not configure a large number of services unless your application requires it. Contact your Cisco account representative for more information.

Important IP Services Gateway functionality is a license-controlled feature. A valid feature license must be installed prior to configuring an IPSG service. Contact your Cisco account representative for more information.

On entering the command with the **radius-server** mode or without any mode, the CLI prompt changes to:

[*context_name*]*hostname*(config-ipsg-service-radius-server)#

On entering the command with the **radius-snoop** mode, the CLI prompt changes to:

[*context_name*]*hostname*(config-ipsg-service-radius-snoop)#

For more information about the IP Services Gateway, refer to the *IP Services Gateway Administration Guide*.

Example

The following command configures an IPSG RADIUS Snoop service named *ipsg1* and enters the IPSG RADIUS Snoop Configuration Mode:

```
ipsg-service ipsg1 mode radius-snoop
```

The following command enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services:

```
ipsg-service ipsg2 mode radius-server ewag
```

ipv6 access-group

Configures the IPv6 Access group.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

ipv6 access-group *group name* **{** *priority_value* **}**

group_name

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

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 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 IPv6 access group name and priority. Use a lower value to indicate a higher priority for the group.

Example

```
ipv6 access-group group_1
```

ipv6 access-list

Create, configure, or delete an IPv6 Access List in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

[no] ipv6 access-list *name*

no

Removes the specified access list.

name

Specifies the access list name.

name is an alphanumeric string of 1 through 47 characters.

If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.

If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

Usage Guidelines Executing this command enters the IPv6 ACL Configuration Mode in which rules and criteria are defined for the ACL.

Important A maximum of 256 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less then 200.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

```
ipv6 access-list samplelist
no ipv6 access-list samplelist
```

ipv6 dns-proxy

Configures the domain name server proxy for the context.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description **[no] ipv6 dns-proxy source-ipv4-address** *ip_address*

no

Removes the predefined IP address for local interface in the destination context.

ip_address

Specifies the IPv4 address of one of the local interface in the destination context to configure the IPv6 DNS proxy where *ip_address* must be specified using IPv4 dotted-decimal notation.

Usage Guidelines The IPv6 DNS proxy source IPv4 address is used as the source IP address for the DNS proxy transaction.

Example

The following command provides an example of configuring a IPv6 DNS proxy of *192.168.23.1*:

```
ipv6 dns-proxy source-ipv4-address 192.168.23.1
```

ipv6 neighbor

Adds a static IPv6 neighbor entry into the neighbor discovery table.

Product

PDIF

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] ipv6 neighbor *ipv6_address hardware_address*

no

Removes the specified address.

ipv6_address hardware_address

ipv6_address is the IP address of node to be added to the table.

hardware_address is the associated 48-bit MAC address.

Usage Guidelines

Add a static IPv6 neighbor entry into the neighbor discovery table.

Important

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

Example

Add the ipv6 address *fe80::210:83ff:fef7:7a9d::/24* and associated 48 bit MAC address *0:10:83:f7:7a:9d* to the table.

```
ipv6 neighbor fe80::210:83ff:fef7:7a9d::/24 0:10:83:f7:7a:9d
```

ipv6 pool

Modifies the current context's IP address pools by adding, updating or deleting a pool. This command also resizes an existing IP pool.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

ipv6 pool *name* **{ 6to4 local-endpoint** *ipv4_address* **[default-relay-router** *router_address* **] | alert threshold | group-name** *name* **| policy { allow-static-allocation | dup-addr-detection } | prefix** *ip_address/len* **[6to4-tunnel local-endpoint** *ip_address* **| default-relay-router** *router_address* **] | range** *start_addressend_address* **| suppress-switchover-arps } [prefix-length** *prfx_length* **] [private** *priority* **] [public** *priority* **] [shared** *priority* **] [static** *priority* **] [group-name** *name* **] [vrf** *vrf-name* **]**
no ipv6 pool *name*

no

Deletes the previously configured IPv6 pool.

name

Specifies the logical name of the IP address pool as an alphanumeric string of 1 through 31 characters.

6to4-tunnel local-endpoint *ip_address*

Specifies the IPv4 address of the local interface to be used for IPv6-to-IPv4 compatible pool address construction.

alert threshold { 6to4 local-endpoint *ipv4_address* | alert threshold | group-available | group-name *name* | policy { allow-static-allocation | dup-addr-detection } | pool-free | pool-used | prefix | range *start_address end_address* }

Default: All thresholds are disabled.

Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IPv6 pool thresholds.

- **6to4**: Sets an alert based on the IPv6 Pool for an IPv6-to-IPv4 compatible address type.
- **alert-threshold**: Sets an alert based on the percentage free alert threshold for this group.
- **group-available**: Sets an alert based on the percentage free alert threshold for this group.

- **group-name**: Sets an alert based on the IPv6 Pool Group.
- **policy allow-static-allocation**: Sets an alert based on the address allocation policy.
- **pool-free**: Sets an alert based on the percentage free alert threshold for this pool.
- **pool-used**: Sets an alert based on the percentage used alert threshold for this pool.
- **prefix**: Sets an alert based on the IPv6 Pool address prefix.
- **range**: Sets an alert based on the IPv6 address pool range of addresses.
- **suppress-switchover-arps**: Sets an alert based on the Suppress Gratuitous ARPs when performing a line card or an MIO switchover.

group name *name*

IPv6 Pool Group.

The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover.

ipv4_address

Specifies the beginning IPv4 address of the IPv4 address pool. *ipv4_address* must be specified using IPv4 dotted-decimal notation.

default-relay-router *router address*

Specifies the default relay router for the tunnel.

policy allow-static-allocation

Allows a dynamic pool to accept a static address allocation.

The following options are available:

- **6to4**: IPv6 Pool for IPv6- to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix

- **range**: Configure IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

policy dup-addr-detection

This command is valid for IPv6 shared pools only (Sample syntax: **ipv6 pool** *name* **prefix** *ip_address/len* **shared policy dup-addr-detection**). When this policy is enabled, the IPv6 shared pool allows a prefix to be shared in different call sessions with different interface IDs for an IPv6 address. This allows the tracking of interface IDs per prefix and the detection of duplicate IDs.

With this policy disabled, the IPv6 shared pool will allow a prefix to be shared across different call sessions. The interface ID is not considered for any duplicate address detection. Default: Disabled

The following options are available:

- **6to4**: IPv6 pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 pool group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

prefix *ip_address/len*

Specifies the beginning IPv6 address of the IPv6 address pool. *ip_address/len* must be specified using IPv6 colon-separated-hexadecimal. *len* is an integer that indicates the number bits of prefix length.

Important If the **prefix** *ip_address/len* specified is less than /40, then a **prefix-length** *prfx_length* must be specified. Options are 48, 52, or 58 bits of **prefix-length**.

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

range *start_address end_address*

Configures an IPv6 address pool to use a range of addresses.

start_address specifies the beginning of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

end_address specifies the end of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

suppress-switchover-arps

Suppresses gratuitous ARPs when performing a line card switchover.

The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

prefix-length *prfx_length*

Specifies a configured length of prefixes. *prfx_length* can be 48, 52, 56 or 64 bits of prefix (Default = 64). This option supports S-GW/P-GW validation of fixed-length addresses via DHCPv6 (TS 29.274 – 7.2.2 and 8.14).

Important If the **prefix** *ip_address/len* specified is less than /40, then a **prefix-length** *prfx_length* must be specified. Options are 48, 52, or 58 bits of **prefix-length**.

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

private *priority* | public *priority* | shared *priority* | static *priority*

Default: **public**

private *priority*: Specifies that the address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest. The default is 0.

public *priority*: Specifies that the address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

shared *priority*: Specifies that the address pool that may be used by more than one session at any time. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

static *priority*: Specifies that the address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

group-name *name*

Groups the IPv6 pools into different groups. The subscribers/domain can be configured with the group-name instead of the prefix-pool names. *name* is the name of the group by which the IPv6 pool is to be configured expressed as an alphanumeric string of 1 through 79 characters.

vrf *vrf-name*

Associates the pool with the VRF specified as an alphanumeric string of 1 through 63 characters. By default the configured IPv6 pool will be associated with the global routing domain.

Usage Guidelines

Use this command to modify the current context's IP address pools by adding, updating or deleting a pool. Also use this command to resize an existing IP pool.

Example

The following command adds an IPv6 pool named *ip6Star*:

```
ipv6 pool ip6Star
```

ipv6 prefix-list

Creates an IPv6 prefix list for filtering routes.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipv6 prefix-list name *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**
no ipv6 prefix-list *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq *seq_number*

Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

any

Matches any prefix.

***network_address/net_mask* [ge *ge_value*] [le *le_value*]**

Specifies the prefix to match.

network_address/net_mask: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal notation. When neither **ge** (greater than or equal to) or **le** (less than or equal to) are specified an exact match is assumed.

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

ge *ge_value*: Specifies the minimum prefix length to match as an integer from 0 through 128. If only the ge value is specified, the range is from the ge value to 128. The ge value must be greater than *net_mask* and less than the le value.

le *le_value*: Specifies the maximum prefix length to match as an integer from 0 through 128. If only the le value is specified, the range is from the *net_mask* to the le value. The le value must be less than or equal to 128.

The following equation describes the conditions that ge and le values must satisfy:

net_mask < *ge_value* < *le_value* <= **128**

Usage Guidelines Use this command to filter routes by their IPv6 prefix.

Example

```
ipv6 prefix-list name prelistv6-10 seq 5 permit 2002::123.45.67.89/32
```

ipv6 prefix-list sequence-number

Enables or disables the inclusion of IPv6 prefix list sequence numbers in the configuration file. This option is enabled by default.

Product PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

[no] ipv6 prefix-list sequence-number

no

Disables the listing of IPv6 prefix list sequence numbers in the configuration file.

Usage Guidelines

Use this command to enable and disable the inclusion of IPv6 prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IPv6 prefix list sequence numbers in the configuration file, enter the following command:

no ipv6 prefix-list sequence-number

ipv6 route

Configures a static IPv6 route to the next-hop router.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

[no] ipv6 route *ipv6_address*/*prefix_length* **{ interface** *name* **| next-hop** *ipv6_address* **interface** *name* **} [cost** *cost***] [fall-over bfd multihop** *mhsess_name* **] [precedence** *precedence* **] [vrf** *vrf_name* **[cost** *value* **] [fall-over bfd multihop** *mhsess_name* **] [precedence** *precedence* **]**
[no] ipv6 route static bfd *if_name remote-endpt_ipv6address*
[no] ipv6 route static multihop bfd *mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr*

no

Removes the specified static route.

ipv6_address/prefix_length

Specifies a destination IPv6 address or group of addresses that will use this route.

ipv6_address/prefix_length must be specified using IPv6 colon-separated-hexadecimal with 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.

interface *name*

Specifies the name of the interface on this system associated with the specified route or next-hop address. *name* must be an existing interface name on the system expressed as an alphanumeric string of 1 through 79 characters.

next-hop *ipv6_address*

The IPv6 address of the directly connected next hop device in IPv6 colon-separated-hexadecimal notation.

cost *cost*

Defines the number of hops to the next gateway as an integer from 0 through 255. Default: 0

fall-over bfd multihop *mhsess_name*

Enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure. Specify *mhsess_name* as an alphanumeric string of 1 through 19 characters.

precedence *precedence*

Indicates the administrative preference of the route. A low precedence specifies that this route takes preference over the route with a higher precedence. *precedence* must be an integer from 1 through 254. Default: 1

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration.

vrf_name is the name of a preconfigured VRF context configured in *Context Configuration Mode* via the **ip vrf** command.

static bfd *if_name remote-endpt_ipv6address*

Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the *BFD Configuration Mode Commands* chapter.

if_name: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.

remote_endpt_ipv6address: Specifies the gateway address of the BFD neighbor in IPv6 colon-separated-hexadecimal notation.

static multihop bfd *mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr*

Creates a static multihop BFD route with local and remote endpoints.

mhbfd_sess_name: Specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.

local_endpt_ipv6addr: Specifies the local endpoint address in IPv6 colon-separated-hexadecimal notation.

remote_endpt_ipv6addr: Specifies the remote endpoint address in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to configure IPv6 route parameters, precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route's being selected first by lower precedence then the cost is used if multiple route's are defined with the same precedence.

This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

Important A maximum of 1,200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Important SNMP traps are generated when BFD sessions go up and down (BFDSessUp and BFDSessDown).

Example

T the following example configures a static route with IPv6 prefix/length *2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24* to the next hop interface *egress1*:

```
ipv6 route 2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 interface egress1
```

ipv6 route-access-list

Configures an IPv6 route access list for filtering routes.

Product

GGSN

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipv6 route-access-list named *list_name* **] { deny | permit }** *network_address*/*net_mask* **[exact-match]**
no ipv6 prefix-list *list_name* **] { deny | permit } { any |** *network_address*/*net_mask* **[exact-match]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

***network_address/net_mask* [exact-match]**

Specifies the prefix to match.

network_address/net_mask: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal 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.

exact-match *le_value*: Specifies that only an exact match will initiate access list deny/permit function.

Usage Guidelines Use this command to filter routes by their IPv6 prefix.

Example

```
ipv6 route-access-list name routelistv6 seq 5 permit 2002::123.45.67.89/24
```

ipv6 rri

Configures Reverse Route Injection (RRI) egress clear port IPv6 parameters. (VPC-VSM only)

Product SecGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipv6 rri { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]
no ipv6 rri { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI egress route.

ipv6_address

Specified in IPv6 colon-separated-hexadecimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines Use this command to configure IPv6 RRI egress clear port IPv6 parameters.

Example

```
ipv6 rri 2001:4A2B::1f3F interface rri03
```

ipv6 rri-route

Configures High Availability (HA) IPv6 routing parameters for Reverse Route Injection (RRI). (VPC-VSM only)

Product SecGW

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipv6 rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ipv6_address* } { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]
no ipv6 rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ipv6_address* } { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI route.

network-mode { L2 | L3 }

Specifies the RRI route network mode type as Layer 2 (L2) or Layer 3 (L3).

clear_loopback_ip

Specifies the loopback address for clear traffic in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

rri-ip *virtual_ipv6_address*

Specifies the use of a virtual IP address on both Primary and Secondary for RRI. *virtual_ipv6_address* is expressed in IPv6 colon-separated-hexadecimal notation.

ipv6_address

Specified in IPv6 colon-separated-hexadecimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure HA IPv6 routing parameters for RRI.

Example

```
ipv6 rri-route network-mode L3 rri-ip 2001:4A2B::1f3F
```

ipv6 sri-route

Configures Layer 3 (L3) High Availability (HA) IPv6 routing parameters for Service Route Injection (SRI). (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

ipv6 sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**
no ipv6 sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**

no

Disables the specified SRI route.

sri-ip *network_address*

Specifies the IPv6 address associated with the SRI route.

next hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure L3 HA IPv6 routing parameters for SRI.

Example

```
ipv6 sri-route sri-ip 2001:4A2B::1f3F interface sri23
```

isakmp disable-phase1-rekey

This command is deprecated. Use **ikev1 disable-phase1-rekey** command to configure the parameters for Phase1 SA rekeying when ISAKMP lifetime expires for IKE v1 protocol.

isakmp keepalive

This command is deprecated. Use **ikev1 keepalive dpd** command to configure ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

isakmp policy

This command is deprecated. Use **ikev1 policy** command to create/configure an ISAKMP policy with the specified priority for IKE v1 protocol.

iups-service

Creates an Iu-PS service instance and enters the Iu-PS Service Configuration Mode. This mode defines the configuration and usage of Iu-PS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN). It defines both the control plane (GTP-C) and the data plane (GTP-U) between these nodes.

Important For details about the commands and parameters for this mode, check the *IuPS Service Configuration Mode Commands* chapter.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description **`[ no ] iups-service`** *`srvc_name`*

no

Remove the configuration for the specified Iu-PS service from the configuration for the current context.

srvc_name

Specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove an Iu-PS service. Add up to eight definitions to be used with a single SGSN service so the SGSN can support multiple PLMNs.

Example

The following command creates an Iu-PS service named *iu-ps1*:

```
iups-service iu-ps1
```

The following command removes the Iu-PS service named *iu-ps1*:

```
no iups-service iu-ps1
```

l2tp peer-dead-time

Configures a delay when attempting to tunnel to a specific peer which is initially unreachable due to reasons such as a network issue or temporarily having reached its capacity.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
l2tp peer-dead-time seconds
default l2tp peer-dead-time
```

default

Rests the command to its default setting of 60.

seconds

Specifies the interval (in seconds) to wait before attempting to tunnel to a specific peer which is initially unreachable as an integer from 5 through 64,000. Default: 60

Usage Guidelines The time to wait before trying to establish a tunnel to a known peer after the initial attempt was unsuccessful.

Example

The following example configures the delay in attempting to tunnel to a temporarily unreachable peer. The delay is set to *120* seconds in this example.

```
l2tp peer-dead-time 120
```

lac-service

Enters the LAC Service Configuration Mode, or is used to add or remove a specified L2TP Access Concentrator (LAC) service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] lac-service *name*

no

Removes the specified lac-service from the current context.

name

Specifies the name of a LAC service to configure, add, or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the LAC Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LAC service named *LAC1* and enter the LAC Service Configuration Mode, enter the following command:

```
lac-service LAC1
```

To configure an existing LAC service named *LAC2*, enter the following command:

```
lac-service LAC2
```

To delete an existing LAC service named *LAC3*, enter the following command:

```
no lac-service LAC3
```

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lawful-intercept dictionary

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

limit ipsecmgr ikev1 max

Use this command to limit the parameter for this context.

Product

IPSec

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

limit ipsecmgr ikev1 max*max_value*

default limit ipsecmgr ikev1 max

default

Sets/Restores default value assigned for specified parameter.

limit

Limits the parameter for this context.

ipsecmgr

To limit ipsecmgr manager settings.

ikev1

Specifies IKEv1 tasks.

max *max_value*

Specifies maximum ipsecmgr IKEv1 tasks. *max_value* must be an integer from 1 to 176.

Example

Use the following command to limit number of IPSec managers within a context to 23.

limit ipsecmgr ikev1 max*23*

lma-service

Creates an Local Mobility Anchor (LMA) service or specifies an existing LMA service and enters the LMA Service Configuration Mode for the current context.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

lma-service *service_name* **[-noconfirm]**
no lma-service *service_name*

no

Removes the specified LMA service from the context.

service_name

Specifies the name of the LMA service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the LMA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution

Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-lma-service)#
```

LMA Service Configuration Mode commands are defined in the *LMA Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: P-GW (SAEGW).

Example

The following command enters the existing LMA Service Configuration Mode (or creates it if it does not already exist) for the service named *lma-service1*:

```
lma-service lma-service1
```

The following command will remove *lma-service1* from the system:

```
no lma-service lma-service1
```

Ins-service

Enters the LNS Service Configuration Mode, or is used to add or remove a specified L2TP Network Server (LNS) service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] lns-service *name*

no

Removes the specified lac-service from the current context.

name

Specifies the name of a LNS service to configure, add or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the LNS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LNS service named *LNS1* and enter the LNS Service Configuration Mode, enter the following commands:

```
lns-service LNS1
```

To configure an existing LNS service named *LNS2*, enter the following command:

```
lns-service LNS2
```

To delete an existing LNS service named *LNS3*, enter the following command:

```
no lns-service LNS3
```

location-service

Creates a location service configuration instance or configures an existing location service configuration and enters the Location Service Configuration Mode. LoCation Services (LCS) are used to determine the geographic location of a UE.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
location-service service_name [ -noconfirm ]
no location-service service_name
     slr emergency unauth-imsi
```

no

Removes the specified location service configuration instance from the context.

service_name

Specifies the name of the location service configuration instance. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

unauth-imsi

Allows MME to send unauthorized IMSI in LRR message when available.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the Location Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing Service Configuration instance.

Location Service Configuration Mode commands are defined in the *Location Service Configuration Mode Commands* chapter.

A maximum of 16 location service instances can be configured per system.

Entering this command results in the following prompt:

```
[context_name]hostname(config-location-service)#
```

Example

The following command enters the existing Location Service Configuration Mode (or creates it if it does not already exist) for the service named *location-service1*:

```
location-service location-service1
```

The following command will remove *location-service1* from the system:

```
no location-service location-service1
```

logging

Modifies the logging options for a specified system log server for the current context.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] logging syslog *ip_address* **[event-verbosity { min | concise | full } | facility** *facilities* **| msg-format { rfc3164 | rfc5424 } | pdu-data { none | hex | hex-ascii } | pdu-verbosity** *pdu_level* **| port** *number* **rate** *value* **] { first-console }**

no

Indicates that internal logging is to be disabled for the options specified.

syslog *ip_address*

Specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

event-verbosity { min | concise | full }

Specifies the level of detail to use in logging of events. Detail level must be one of the following:

- **min**: Displays minimal detail.
- **concise**:Displays summary detail.
- **full**: Displays full detail.

facility *facilities*

Default: **local7**

Specifies the local facility for which the system logging server's logging options shall be applied. Local facility must be one of the following:

- **local0** — Pertains to syslog severity level of 0, Emergency
- **local1** — Pertains to syslog severity level of 1, Alert
- **local2** — Pertains to syslog severity level of 2, Critical
- **local3** — Pertains to syslog severity level of 3, Error
- **local4** — Pertains to syslog severity level of 4, Warning

- **local5** — Pertains to syslog severity level of 5, Notice
- **local6** — Pertains to syslog severity level of 6, Informational
- **local7** — Pertains to syslog severity level of 7, Debug

If local facility is not specified, then **local7** is applied by default.

Multiple system log servers can share the logging options of a given local facility. This allows for the logical grouping of system log servers and the options which affect all of those associated with the same local facility.

msg-format { rfc3164 | rfc5424 }

Configures the message format for each system log server as per RFC3164 or RFC5424. Default: rfc3164.

pdu-data { none | hex | hex-ascii }

Specifies output format for packet data units when logged. Format must be one of the following:

- **none**: Displays data in raw format.
- **hex**: Displays data in hexadecimal format.
- **hex-ascii**:Displays data in hexadecimal and ASCII format (similar to a main-frame dump).

pdu-verbosity *pdu_level*

Specifies the level of verboseness to use in logging of packet data units as a value from 1 through 5, where 5 is the most detailed.

port *number*

Specifies an alternate port number for the system log server. Default: 514.

number must be an integer value from 1 through 65535.

rate *value*

Specifies the rate at which log entries are allowed to be sent to the system log server. No more than the number specified by *value* will be sent to a system log server within any given one-second interval.

value must be an integer from 0 through 100000. Default: 1000

first-console

Enables the first serial port as the debug console for event log collection.

Note that on a VPC-DI that has a CF and SF card, the CF card on the first serial port is configured as the debug console. The second serial port is configured as the CLI console.

Note The CF card on the VPC-DI and VPC-SI can be configured as the VGA, which also provides the CLI console.

On the SF card, the first serial port is configured as the debug console. The second serial port cannot be configured as the CLI console because there is no support for this console on the SF card.

Note The **logging first-console** CLI command does not enable or disable system logs such as crash logs, system printed logs, and so on, which are always enabled.

Usage Guidelines Set the log servers to enable remote review of log data.

Example

The following sets the logging for events to the maximum for the local7 facility:

```
logging syslog 10.2.3.4 event-verbosity full
```

The following command sets the logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii for the local3 facility:

```
logging syslog 10.2.3.4 facility local3 pdu-data hex-ascii pdu-verbosity
 3
```

The following sets the rate of information for the local1 facility:

```
logging syslog 10.2.3.4 facility local1 rate 100
```

The following disables internal logging to the system log server specified:

```
no logging syslog 10.2.3.4
```

The following configure the first serial port as the debug console:

```
logging first-console
```

mag-service

Creates a Mobile Access Gateway (MAG) service or specifies an existing MAG service and enters the MAG Service Configuration Mode for the current context.

Product HSGW

S-GW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mag-service service_name [ -noconfirm ]
no mag-service service_name
```

no

Removes the specified MAG service from the context.

service_name

Specifies the name of the MAG service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the MAG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mag-service)#
```

MAG Service Configuration Mode commands are defined in the *MAG Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: HSGW and S-GW.

Example

The following command enters the existing MAG Service Configuration Mode (or creates it if it does not already exist) for the service named *mag-service1*:

```
mag-service mag-service1
```

The following command will remove *mag-service1* from the system:

```
no mag-service mag-service1
```

map-service

Creates a Mobile Application Part (MAP) Service instance and enters the MAP Service Configuration mode to define or edit the MAP service parameters.

MAP is the SS7 protocol that provides the application layer required by some of the nodes in GPRS/UMTS networks to communicate with each other in order to provide services to mobile phone users. MAP is used by the serving GPRS support node (SGSN) to access SS7 network nodes such as a home location register (HLR) or a radio access network (RAN).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

map-service *srvc_name*
no map-service *srvc_name*

no

Remove the specified MAP service from the configuration for the current context.

srvc_name

Specifies the name of the MAP service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove a MAP service configuration.

Important For details about the commands and parameters, check the *MAP Service Configuration Mode Commands* chapter.

Example

The following command creates a MAP service named *map_1*:

```
map-service map_1
```

The following command removes the configuration for a MAP service named *map_1* from the configuration for the current context:

```
no map-service map_1
```

max-sessions

Configures the maximum simultaneous sessions allows for corresponding users.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

max-sessions number { administrator name *user_name* **| config-administrator name** *user_name* **| inspector name** *user_name* **| operator name** *user_name* **}**
no max-sessions { administrator name *user_name* **| config-administrator name** *user_name* **| inspector name** *user_name* **| operator name** *user_name* **}**
default max-sessions { administrator name *user_name* **| config-administrator name** *user_name* **| inspector name** *user_name* **| operator name** *user_name* **}**

max-sessions *number*

Specifies the maximum number of simultaneous CLI sessions. It must be an alphanumeric integer from 1 to 100. **Default**: No limit.

administrator

Configures login user with security administrator rights for specific content. A username must follow the **administrator** keyword.

config-administrator

Configures login user with configuration administrator rights for specific content. A username must follow the **config-administrator** keyword.

inspector

Configures login user with inspector rights for specific content. A username must follow the **inspector** keyword.

operator

Configures login user with operator rights for specific content. A username must follow the **operator** keyword.

name *user_name*

Specifies the username. *user_name* specifies the security username. It must be an string size from 1 to 32.

no

Removes the configured maximum number of simultaneous CLI sessions. This option returns the user to the default setting. If the user does not exist, then an error message appears stating: 'Failure: User x has not been configured. Configure it first!'.

default

Removes the configured maximum number of simultaneous CLI sessions and returns the user to the default number. **Default**: No limit.

Usage Guidelines

This command allows administrative users the ability configure the maximum simultaneous sessions allowed for corresponding users.

Example

The following command allows an administrator the ability to configure 4 simultaneous sessions for user 5.

max-sessions 4 administrator name 5

mipv6ha-service

Creates a Mobile IPv6 Home Agent (MIPv6-HA) service instance and enters the MIPv6 HA Service Configuration mode to define or edit the MIPv6-HA service parameters.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

mipv6ha-service *srvc_name*
no mipv6ha-service *srvc_name*

no

Remove the specified MIPv6-HA service from the configuration for the current context.

srvc_name

Specifies the name of the MIPv6-HA service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove a MIPv6-HA service configuration.

Important For details about the commands and parameters, check the *MIPv6 HA Service Configuration Mode Commands* chapter.

Example

The following command creates a MIPv6-HA service named *mipv6ha_1*:

```
mipv6ha-service mipv6ha_1
```

The following command removes the configuration for a MIPv6-HA service named *mipv6ha_1* from the configuration for the current context:

```
no mipv6ha-service mipv6ha_1
```

mme-embms-service

Creates an MME-eMBMS service or configures an existing MME-eMBMS service. As well, this command enters the MME-eMBMS Service configuration mode. MME-eMBMS service handles the MME's Multimedia Broadcast/Multicast Service (MBMS) functional for Evolved Packet Core (EPC) networks in the current context.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mme-embms-service service_name [ -noconfirm ]
no mme-embms-service service_name
```

no

Removes the specified MME-eMBMS service from the context.

service_name

Specifies the name of the MME-eMBMS service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines Enter the MME-eMBMS Service configuration mode to access the commands needed to setup or modify either a newly defined service or an existing service. This command is also used to remove an existing MME-eMBMS service from the MME's configuration.

A maximum of 8 MME-eMBMS services can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mme-embms-service)#
```

MME Service Configuration Mode commands are defined in the *MME Service Configuration Mode Commands* chapter.

Example

The following command enters the existing MME-eMBMS Service configuration mode (or creates it if it does not already exist) for the service named *embms1*:

```
mme-embms-service embms1
```

The following command will remove *embms1* from the system:

```
no mme-embms-service embms1
```

mme-service

Creates an Mobility Management Entity (MME) service or configures an existing MME service and enters the MME Service Configuration Mode for Evolved Packet Core (EPC) networks in the current context.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mme-service service_name [ -noconfirm ]
no mme-service service_name
```

no

Removes the specified MME service from the context.

service_name

Specifies the name of the MME service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the MME Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 8 MME service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mme-service)#
```

MME Service Configuration Mode commands are defined in the *MME Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The MME service cannot be configured without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

Example

The following command enters the existing MME Service Configuration Mode (or creates it if it does not already exist) for the service named *mme-service1*:

```
mme-service mme-service1
```

The following command will remove *mme-service1* from the system:

```
no mme-service mme-service1
```

mobile-access-gateway

Controls whether duplicate MAG sessions are allowed in HSGW. By default, duplicate sessions are rejected.

Product

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mobile-access-gateway newcall duplicate-session { purge | reject }
[ default | no ] mobile-access-gateway newcall duplicate-session
```

default | no

Disables the feature. New session create request is discarded.

newcall duplicate-session { purge | reject }

Determines new call related behavior on context when duplicate MAG sessions are requested in HSGW (Mobile Access Gateway).

purge: Enables the feature. Old MAG session is deleted and new session create request is rejected, but on retry the new call comes up.

reject: Disables the feature. Rejects new call with duplicate session create request; new session create request is discarded.

Usage Guidelines

This command controls whether duplicate MAG sessions are allowed in HSGW.

When enabled, HSGW rejects new session create request initially and creates new call on retry.

When disabled, HSGW rejects new call and new session create request is discarded.

Example

The following command allows duplicate MAG sessions in HSGW on this context:

mobile-access-gateway newcall duplicate-session purge

mobile-ip fa

Configures settings that effect all FA services in the current context.

Product

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mobile-ip fa { multiple-dynamic-reg-per-nai | newcall
duplicate-home-address { accept | reject } }
{ default | no } mobile-ip fa { multiple-dynamic-reg-per-nai | newcall
duplicate-home-address }
```

default

Configures the default setting for the specified parameter.

- **multiple-dynamic-reg-per-nai**:All FA services in the current context can not simultaneously setup multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: **reject**

no

- **multiple-dynamic-reg-per-nai**: Disables all FA services in the current context from simultaneously setting up multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**:Resets this option to its default of reject.

multiple-dynamic-reg-per-nai

This keyword allows all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI.

newcall duplicate-home-address { accept | reject }

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

Usage Guidelines

Use this command to set the behavior of all FA services in the current context.

Example

To configure all FA services to accept new calls and drop the existing call when the new call requests an IP address that is already in use by an existing call, enter the following command:

```
mobile-ip fa newcall duplicate-home-address accept
```

To enable all FA services in the current context to allow all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI, enter the following command:

```
mobile-ip fa multiple-dynamic-reg-per-nai
```

mobile-ip ha assignment-table

Creates a Mobile IP HA assignment table and enters Mobile IP HA Assignment Table Configuration Mode.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

mobile-ip ha assignment-table *atable_name* **[-noconfirm]**
no mobile-ip ha assignment-table *atable_name*

no

This keyword deletes the specified assignment table

atable_name

Specifies the name of the MIP HA assignment table to create or edit as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create a new MIP HA assignment table or edit an existing MIP HA assignment table.

Important

A maximum of eight MIPHA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.

Important A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

Example

The following command creates a new MIP HA assignment table name *MIPHAtable1* and enters MIP HA Assignment Table Configuration Mode without asking for confirmation from the user:

```
mobile-ip ha assignment-table MIPHAtable1
```

mobile-ip ha newcall

Configures the behavior of all HA services when duplicate home addresses and duplicate IMSI sessions occur for new calls.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

```
mobile-ip ha newcall { duplicate-home-address { accept | reject } |
duplicate-imsi-session { allow | disallow | global-disallow } |
wimax-session-overwrite { allow | disallow }
{ default | no } mobile-ip ha newcall { duplicate-home-address |
duplicate-imsi-session | wimax-session-overwrite }
```

default

Configures the default setting for the specified parameter.

- **duplicate-home-address**: **reject**—sets HA services to reject a new call that requests an IP address that is already assigned.
- **duplicate-imsi-session**: **allow**—sets HA services to accept new calls that have the same IMSI as a call that is already active.
- **wimax-session-overwrite:disallow**—disable session overwrite feature for WiMax mobile-ip calls on the HA.

no

Configures the default setting for the specified parameter.

duplicate-home-address { accept | reject }

Configures the HA to either accept or reject new calls if the new call requests a static IP home address that is already assigned to an existing call from an IP address pool in the same destination context.

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

duplicate-imsi-session { allow | disallow | global-disallow }

Configures the HA to either permit or not permit multiple sessions for the same IMSI.

- **allow**: Allows multiple sessions for the same IMSI.
- **disallow**: If a mobile node already has an active session and a new sessions is requested using the same IMSI, the currently active session is dropped and the new session is accepted.
- **global-disallow**: Enables HA services in this context to accept a new session and disconnect any other session(s) having the same IMSI being processed in this context. In addition, a request is sent to all other contexts containing HA services to do the same.

Important In order to ensure a single session per IMSI across all contexts containing HA services, the global-disallow option must be configured in every context.

wimax-session-overwrite { allow | disallow }

Use this command to enable or disable the overwrite feature for WiMAX mobile ip (MIPv4) calls on the HA.

Usage Guidelines Use this command to set the behavior of all HA services for new calls.

Example

To configure all HA services to accept new calls when the new call requests a static IP that is already assigned from an IP pool in the same destination context, enter the following command:

```
mobile-ip ha newcall duplicate-home-address accept
```

To configure all HA services to drop an active call and accept a new one that uses the same IMSI, enter the following command:

```
mobile-ip ha newcall duplicate-imsi-session disallow
```

mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product HA

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

`[ no ] mobile-ip ha reconnect [ static-homeaddr [ dynamic-pool-allocation ] ] }`

static-homeaddr

Specifies that the home address as a static IP address.

dynamic-pool-allocation

Allows a dynamic pool to accept a static address allocation.

Usage Guidelines

Use this command to reset the HA behavior for new calls.

Example

```
mobile-ip ha reconnect
mobile-ip ha reconnect static-homeaddr
mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation
no mobile-ip ha reconnect
no mobile-ip ha reconnect static-homeaddr
```

monitor-protocols

Enters the Monitor Protocols configuration mode.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

`monitor-protocols`

Usage Guidelines

The Monitor Protocols configuration mode contains commands used to configure protocol monitoring groups (relationships) between the current device and a remote peer.

Configure monitor protocol groups on both the CP and UP and within the same context as the CUPS Sx interface.

mpls bgp forwarding

Globally enables Multi protocol Label Switching (MPLS) Border Gateway Protocol (BGP) forwarding.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

Syntax Description

`[ no ] mpls bgp forwarding`

no

Disables MPLS BGP forwarding.

Usage Guidelines

Use this command to globally enable the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LSP to forward the IP packets. If this command is not enabled, then the nexthop for the BGP routes must be reachable via LDP.

Caution This command should always be enabled when nexhtop is not reachable thorough LSP.

Example

The following command enables the MPLS BGP forwarding on the system:

`mpls bgp forwarding`

mpls exp

Sets the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP (Experimental) header. This setting overrides the value sent by the mobile subscriber.

Product

eHRPD

GGSN

PDSN (HA)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] mpls exp *<value>*

no

Reverts back to the default behavior, which is to copy the DSCP from the mobile subscriber packet to the EXP header of the packet, if there is no explicit configuration for DSCP to EXP.

<value>

Specifies the MPLS EXP header value as an integer from 0 through 7. Higher value indicates higher priority.

Usage Guidelines

Set the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP header. This value applies to all the VRFs in the context. The default behavior is to copy the DSCP value of mobile subscriber traffic to the EXP header, if there is no explicit configuration for DSCP to EXP (via the **mpls map-dscp-to-exp dscp** <*n*> **exp** <*m*> command).

This command disables the default behavior and sets the EXP value to the configured <value>.

Example

The following command sets the MPLS EXP header value to 2:

```
mpls exp 2
```

mpls ip

Globally enables the Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths.

Product

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] mpls ip

no

Disables MPLS forwarding of IPv4 packets configured on the system. **no mpls ip** stops dynamic label distribution on all the interfaces regardless of interface configuration.

Usage Guidelines

Globally enables the MPLS forwarding of IPv4 packets along normally routed paths for the entire context.

It does not start label distribution over an interface until MPLS has been enabled for the interface as well. Refer to the *Ethernet Interface Configuration Mode Commands* chapter for additional information.

Caution This feature is not enabled by default.

Example

Following command enables (but does not start) MPLS forwarding of IPv4 packets along normally routed paths:

```
mpls ip
```

mseg-service

This command is not supported in this release.

multicast-proxy

Creates, configures or deletes a multicast proxy host configuration.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax Description

[no] multicast-proxy { igmp interface *ip_address* **range-start** *start_ip_address* **range-end** *end_ip_address* **| listen address** *listen_ip_address* **port** *port_number* **protocol** *protocol_number* **sessmgr** *instance* **}**

no

If previously configured, deletes the specified multicast proxy parameter from the current context.

igmp interface *ip_address* range-start *start_ip_address* range-end *end_ip_address*

Specifies the IP address and range of associated addresses for this Internet Group Management Protocol (IGMP) interface.

ip_address is the IP address of this interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

range-start *start_ip_address* is the start point for the multicast address range expressed in IPv4dotted-decimal or IPv6 colon-separated-hexadecimal notation.

range-end *end_ip_address* is the end point for the multicast address range expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *end_ip_address*

listen address *listen_ip_address* port *port_number* protocol *protocol_number* sessmgr *instance*

Configures this context as a multicast proxy listener.

listen_ip_address is the IP address that will be listened to, expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number* is the port number which will be listened to. If this is not provided, the listener will receive all packets from the *listen_ip_address*. *port_number* is an integer from 1 through 65535.

protocol *protocol_number* is the IANA protocol number associated with the port number. If this is not provided, the listener will receive all packets from the *listen_ip_address* and *port_number*. *protocol_number* is an integer from 1 through 255.

sessmgr *instance* session manager instance that will do the listening. *instance* is an integer from 1 through 270.

Usage Guidelines

Use this command to create/configure/delete a multicast proxy host configuration.

Example

The following command creates an IGMP multicast host configuration:

```
multicast proxy igmp interface 192.155.1.34 range-start 255.0.0.0 range-end
 255.0.0.1
```