

HA Service Configuration Mode Commands

The HA Service Configuration Mode is used to create and manage the Home Agent (HA) services within the current context.

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

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

- a11-signalling-packets, on page 2
- aaa, on page 3
- access-network, on page 4
- associate, on page 5
- authentication, on page 6
- bind, on page 8
- binding-update, on page 9
- default, on page 10
- default subscriber, on page 12
- description, on page 13
- encapsulation, on page 14
- end, on page 15
- exit, on page 15
- fa-ha-spi, on page 15
- gre, on page 17
- idle-timeout-mode, on page 19
- ikev1, on page 20
- ip context-name, on page 21
- ip local-port, on page 22
- ip pool, on page 22
- isakmp, on page 23

- min-reg-lifetime, on page 25
- mn-ha-spi, on page 26
- nat-traversal, on page 28
- optimize tunnel-reassembly, on page 29
- per-domain statistics-collection, on page 29
- policy bc-query-result, on page 30
- policy nw-reachability-fail, on page 31
- policy overload, on page 32
- policy null-username, on page 34
- private-address allow-no-reverse-tunnel, on page 35
- radius accounting dropped-pkts, on page 35
- reg-lifetime, on page 36
- reverse-tunnel, on page 37
- revocation, on page 38
- setup-timeout, on page 40
- simul-bindings, on page 41
- threshold dereg-reply-error, on page 42
- threshold init-rrq-rcvd-rate, on page 43
- threshold ipsec-call-req-rej, on page 44
- threshold ipsec-ike-failrate, on page 45
- threshold ipsec-ike-failures, on page 46
- threshold ipsec-ike-requests, on page 48
- threshold ipsec-tunnels-established, on page 49
- threshold ipsec-tunnels-setup, on page 50
- threshold reg-reply-error, on page 51
- threshold rereg-reply-error, on page 52
- wimax-3gpp2 interworking, on page 53

a11-signalling-packets

Applies Differentiated Services Code Point (DSCP) marking for IP headers carrying outgoing signalling packets.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

a11-signalling-packets ip-header-dscp *ip-header-dscp*
{ default | no } a11-signalling-packets ip-header-dscp

no

Disables DSCP marking for IP header encapsulation for the HA service.

default

Configures DSCP marking for IP header encapsulation for a specific HA service.

ip-header-dscp

Is a hexadecimal number between 0x0 and 0x3F.

Usage Guidelines Use this command to apply DSCP marking for IP header carrying outgoing signalling packets.

Example

The following command applies DSCP marking for IP header carrying outgoing signalling packets.

a11-signalling-packets ip-header-dscp 0x2f

aaa

Configures the sending of subscriber session AAA accounting by the HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

```
aaa { accounting [ roaming ] | group string }
no aaa { accounting | group }
default aaa accounting
```

no

Disables AAA accounting for the HA service.

default

Configures AAA parameters for specific HA service

accounting

accounting Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA), by default is enabled.

roaming Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA) only for roaming subscribers.

group

group configures aaa group for ha-service, **group** has lower priority than subscriber/apn config.

string: size ranges between *1* and *63*.

Usage Guidelines

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.

The chassis is shipped from the factory with the AAA accounting enabled.



Important In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the aaa accounting subscriber radius command.

Example

The following command disables aaa accounting for the HA service:

```
no aaa accounting
```

access-network

Configures a specific access network configuration.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

access-network accounting identifier *access_network_accounting_identifier*
no access-network accounting identifier

no

Disables a specific access network configuration.

accounting

Specifies an access network configuration for accounting

identifier

Specifies an access network accounting identifier

access_network_accounting_identifier

This is an alphanumeric string of 1 through 128 characters.

Usage Guidelines This command is used to configure an access network for accounting.

Example

The following command configures an access network for accounting with the identifier *idnt*:

access-network accounting identifier idnt

associate

Associates an HA-service with a QoS policy.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

`associate qci-qos-mapping` *`string`*
`no associate qci-qos-mapping`

no

Disables the association of an HA-service with a QoS policy.

qci-qos-mapping*string*

Maps a QoS Class Identifier (QCI) for this HA service.

string is an alphanumeric string of 1 through 63 characters.

Usage Guidelines This command associates an HA-service with a QoS policy.

Example

The following command associates an HA-service with a QCI *map01*.

associate qci-qos-mapping map01

authentication

Configures authentication parameters for a specific HA service within a context.

Product

HA

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
authentication { aaa-distributed-mip-keys [ disabled | optional | required
 ] | dmu-refresh-key | imsi-auth| mn-aaa { allow-noauth | always|
dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth } |
mn-ha { allow-noauth | always } | pmip-auth | stale-key-disconnect }
no authentication { imsi-auth | pmip-auth }
default authentication { aaa-distributed-mip-keys | dmu-refresh-key |
imsi-auth | mn-aaa | mn-ha | pmip-auth | stale-key-disconnect }
```

no

Disable the parameter.

default

Resets the specified option to its default setting.

aaa-distributed-mip-keys [disabled | optional |required]

Configures use of AAA distributed MIP keys for authenticating RRQ for WiMAX HA calls.

Default is disabled.

disabled: Disables using AAA distributed WiMAX Mobile IP (MIP) keys for authenticating MIP RRQ.

optional: Uses AAA distributed WiMAX MIP keys for authenticating RRQ with fallback option to use static/3GPP2 based MIP keys.

required: AAA distributed WiMAX MIP keys for authenticating MIP RRQ are mandatory

dmu-refresh-key

Typically, when a Dynamic Mobile IP Update (DMU) resets, the next MIP re-registration causes MN-HA authorization failure and the HA rejects the MIP RRQ. This parameter enables the HA to retrieve the MN-HA key again from the AAA during the call and to use the freshly retrieved key value to recheck authentication.

Default is disabled.

imsi-auth

Enable uses the International Subscriber Mobile identity (IMSI) to determine if MN-AAA or MN-FAC extensions are not present in the RRQ.

Default is disabled.

mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth }

Specifies how mobile node-to-AAA authentication extension in registration requests from the mobile node should be handled by the HA service.

Default is always.

allow-noauth: Specifies that the HA service does not require authentication for every mobile node registration request. However, if the mn-aaa extension is received, the HA service will authenticate it.

always: Specifies that the HA service will perform authentication each time a mobile node registers.

dereg-noauth: Disables authentication request upon de-registration.

noauth: Specifies that the HA service will not look for mn-aaa extension and will not authenticate it.

renew-reg-noauth: Specifies that the HA service will not perform authentication for mobile node re-registrations. Initial registration and de-registration will be handled normally.

renew-and-dereg-noauth: Disables authentication request upon re-registration and de-registration.

mn-ha { allow-noauth | always }

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.

Default is always.

allow-noauth: Allows a request that does not contain the auth extension.

always: A request should always contain the auth extension to be accepted.

pmip-auth

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.

Default is always.

allow-noauth: Allows a request that does not contain the auth extension.

always: A request should always contain the auth extension to be accepted.

stale-key-disconnect

If MN-HA auth fails for MIP renew and dereg, disconnects the call immediately.

Disabled by default.

Usage Guidelines

The **authentication** command, combined with a keyword, can be used to specify how the system will perform authentication of registration request messages.

Example

The following command configures the HA service to always perform mobile node authentication for every registration request.

authentication mn-aaa always

The following command configures the HA service to always look for an MN-HA authentication extension in the RRQ.

authentication mn-ha always

bind

Binds the HA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
bind address { range_IPv4address ip_mask | range_IPv4address/bitmask } [
max-subscribers count ]
no bind address
```

range_IPv4address ip_mask | range_IPv4address/bitmask

Specifies the pool of IP addresses (in IPv4 dotted-decimal notation) of the interface configured as the Pi interface with an enterprise HA (EHA). *ip_mask* and *bitmask* specifies the number of subnet bits, representing the subnet mask in CIDR notation and must be a value between 1 to 32.

range_IPv4address is a preconfigured range of IPv4 addresses in Loopback Interface Configuration Mode to enable the Enterprise HA support with enhanced capacity and configured

max-subscribers *count*

Default: *2500000*

Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to an integer from 0 through 4000000.



Important The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system.

Usage Guidelines

Associate the HA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces that you will configuring for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

IP range support is provided through *ranged_address* value. This value enables the pool of IPv4 addresses to support Enterprise HA on HA service to connect enhanced number of enterprise nodes. Refer *HA Administration Guide* for more information.

Use the **no bind address** command to delete a previously configured binding.

Example

The following command would bind the logical IP interface with the address of *209.165.201.1* to the HA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 209.165.201.1
max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

The following command binds the range of IP addresses with HA service to be used with Enterprise HA support:

```
bind address 209.165.201.0/24
```

binding-update

Configures MIP binding-update message related parameters.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

binding-update { max-retransmission *num* **| retransmission-timeout** *seconds* **}**

max-retransmission *num*

Default *3*.

Configures the number of times the message shall be transmitted. *num* must be an integer from 1 through 5.

retransmission-timeout *seconds*

Default 2.

Configures the transmission timeout for the message in seconds. *seconds* must be an integer from 1 through 60.

Usage Guidelines

Configure binding update parameters.

Example

Set the maximum number of times a MIP binding update message is transmitted to *4* with the following command:

```
binding-update max-retransmission 4
```

default

Restores default values assigned for a specified parameter.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
default { authentication { imsi-auth | mn-aaa | mn-ha } | binding-update
 { max-retransmission | retransmission-timeout } | encapsulation | gre {
 checksum | checksum-verify | reorder-timeout | sequence-mode |
sequence-numbers } | ip local-port | policy { null-username |
nw-reachability-fail | overload } | private-address allow-no-reverse-tunnel
 | reg-lifetime | reverse-tunnel | revocation [ enable | max-retransmission
 | retransmission-timeout | trigger handoff ] | setup-timeout |
simul-bindings }
```

authentication

imsi-auth: Restores IMSI authentication to its default: disabled.

mn-aaa: Restores the Foreign Agent (FA) mobile node re-registration authentication setting to its default: always.

mn-ha: Configures the HA service to its default behavior of looking for an MN-HA authentication extension in the RRQ.

binding-update { max-retransmission | retransmission-timeout }

Sets the MIP binding-update message related parameters to their defaults.

max-retransmission: Default 3.

Configures the number of times the message shall be transmitted to 3.

retransmission-timeout: Configures the transmission timeout for the message to 2 seconds.

encapsulation

Sets MIP data encapsulation using GRE to its default: enabled.

gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers }

Sets default Generic Routing Encapsulation (GRE) parameters.

checksum: Disables the introduction of the checksum field in outgoing GRE packets.

checksum-verify: Disables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout: Sets the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to the default setting: 100.

sequence-mode: Disables the reordering of incoming out-of-sequence GRE packets by setting this parameter to the default setting: none.

sequence-numbers: Disables the insertion or removal of GRE sequence numbers in GRE packets.

ip local-port

Restores the IP local-port setting to its default: 434.

policy { null-username | nw-reachability-fail | overload }

Restores the Home Agent service session policy settings.

null-username: Rejects all RRQs that do not have an NAI.

nw-reachability-fail: If the network is not reachable, rejects all incoming sessions.

overload: Restores the Home Agent service session overload policy setting to its default: reject.

private-address allow-no-reverse-tunnel

Resets the HA so that it does not accept MIP calls that use a private address without reverse tunneling.

reg-lifetime

Restores the Mobile IP session registration lifetime setting configured by the **reg-lifetime** command to its default: 600 seconds.

reverse-tunnel

Restores the reverse tunneling setting to its default: enabled.

revocation [enable | max-retransmission | retransmission-timeout | trigger { handoff | idle-timeout}]

Resets the MIP Registration Revocation settings to their default values. When no optional keywords are specified all revocation settings are set to their defaults.

enable: Disables MIP Registration Revocation on the FA.

max-retransmission: Sets the maximum number of retransmissions to 3.

retransmission-timeout: Sets the retransmission timeout to 3 seconds.

trigger { handoff | idle-timeout }: **handoff** enables inter-Access Gateway/FA handoff as a trigger for MIP Registration Revocation. **idle-timeout** enables session idle timer expiration as a trigger for MIP Registration Revocation.

setup-timeout

Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.

simul-bindings

Restores the simultaneous bindings setting to its default: 3.

Usage Guidelines

After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Example

The following command is used to return the IP local-port parameter to its default value:

```
default ip local-port
```

default subscriber

Specifies the name of a subscriber profile configured within the same context as the HA service from which to base the handling of all other subscriber sessions handled by the HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

[no] default subscriber *profile_name*

profile_name

Specifies the name of the configured subscriber profile. *profile_name* is an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage Guidelines

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.

By default, the HA service will use the information configured for the subscriber named default within the same context. This command allows for multiple HA services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the **no default subscriber** *profile_name* command to delete the configured default subscriber.

Example

To configure the HA service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

description *text*
no description

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.

encapsulation

Configures Mobile IP (MIP) encapsulation types supported for a specific HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

`[ no ] encapsulation allow { gre | keyless-gre }`

no

Disables MIP encapsulation types supported for specific HA service

allow

Allows encapsulation type for MIP data.

gre

Default: Enabled.

Specifies the use of Generic Routing Encapsulation (GRE) for MIP data.

keyless-gre

Default: Disabled.

Specifies the use of GRE without exchanging keys for MIP data.

Usage Guidelines

Use to disable or re-enable the use of GRE encapsulation or Key-less encapsulation for MIP sessions.

In case of chassis HA operating with other vendor equipment, which does not support the 3GPP2 to exchange key, this command with **keyless-gre** keyword will make the chassis HA to accept MIP data with legacy GRE.

Example

To disable GRE for MIP sessions, enter the following command:

```
no encapsulation allow
gre
```

To re-enable GRE for MIP sessions, enter the following command:

```
encapsulation allow
gre
```

To enable key-less GRE for MIP sessions, enter the following command:

```
encapsulation allow
keyless-gre
```

end

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

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

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

exit

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

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

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

fa-ha-spi

Configures the security parameter index (SPI) for specific HA service parameters.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description **fa-ha-spi remote-address {** *fa_ip_address* **|** *fa_ip_address_mask* **} spi-number** *number* **{ encrypted secret** *enc_secret* **| secret** *secret* **} [allow-fa-ha-auth-extension] [description** *string* **] [disallow-fa-ha-auth-extension] [hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }] [replay-protection { nonce | timestamp [timestamp-tolerance tolerance] }] [timestamp-tolerance** *tolerance* **]**

no fa-ha-spiremote-address { *ha_ip_address* | *ha_ip_address/mask* } spi-number *number*

no

Disables the security parameter index (SPI) for specific HA service parameters.

remote-address { *fa_ip_address* | *fa_ip_address/mask* }

Specifies the IP address of the FA. *fa_ip_address* is entered using IPv4 dotted-decimal notation with CIDR for the subnet mask.



Important The system supports unlimited peer FA addresses per HA but only maintains statistics for a maximum of 8,192 peer FAs. If more than 8,192 FAs are attached, older statistics are overwritten.

spi-number *number*

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with RFC 2002.

number is an integer value from 256 through 4294967295.

encrypted secret *enc_secret* | secret *secret*

Configures the shared-secret between the HA service and the FA. The secret can be either encrypted or non-encrypted.

encrypted secret *enc_secret*: Specifies the encrypted shared key between the HA service and the FA. *enc_secret* must be an alphanumeric string of 1 through 236 characters that is case sensitive.

secret *secret*: Specifies the shared key between the HA service and the FA. *secret* must be an alphanumeric string of 1 through 236 characters that is case sensitive.

allow-fa-ha-auth-extension

Allows validation of FA HA Authentication extension.

description *string*

This is a description for the SPI. *string* must be an alphanumeric string of 0 through 31 characters.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5

Specifies the hash-algorithm used between the HA service and the FA.

hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.

md5: Configures the hash-algorithm to implement MD5 per RFC 1321.

rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { timestamp [timestamp-tolerance tolerance] | nonce }

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.

nonce: Configures replay protection to be implemented using NONCE per RFC 2002.

timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance: Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. *tolerance* is measured in seconds and can be configured to an integer from 1 and 65535. The default is 60.

Usage Guidelines

An SPI is a security mechanism configured and shared by the HA service and the FA. Please refer to RFC 2002 for additional information.

Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a "default" SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.



Important The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per HA service.

Use the **no** version of this command to delete a previously configured SPI.

Example

The following command configures the FA service to use an SPI of *512* when communicating with an HA with the IP address *209.165.200.226*. The key that would be shared between the HA and the FA service is *q397F65*. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```
fa-ha-spi remote-address 209.165.200.226 spi-number 512 secret q397F65
hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of *209.165.202.128*:

```
no fa-ha-spi remote-address 209.165.202.128 spi-number 400
```

gre

Configures Generic Routing Encapsulation (GRE) parameters.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode
 { none | reorder } | sequence-numbers }
default gre { checksum | checksum-verify | reorder-timeout | sequence-mode
 | sequence-numbers }
no gre { checksum | checksum-verify | sequence-numbers }
```

no

Disables the specified functionality.

default

Sets or restores default value assigned for specified parameter.

checksum

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout *timeout*

Default: 100

Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *timeout* must be an integer from 0 through 5000.

sequence-mode { none | reorder }

Default: none

Configures how incoming out-of-sequence GRE packets should be handled.

none: Disables reordering of incoming out-of-sequence GRE packets.

reorder: Enables reordering of incoming out-of-sequence GRE packets.

sequence-numbers

Default: Disabled

Enables the insertion of sequence numbers into the GRE packets.

Usage Guidelines

Use this command to configure how the HA service handles GRE packets.

Example

To set the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to *500* milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```

To enable the insertion or removal of GRE sequence numbers in GRE packets, enter the following command:

```
gre sequence-numbers
```

idle-timeout-mode

Configures the sessions idle-timer reset behavior.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
idle-timeout-mode { aggressive | handoff | normal } [ upstream-only ]
default idle-timeout-mode
```

default

Resets the idle timeout mode to the default settings.

aggressive

Resets the session idle timer only when MIP user data is detected. This is the default behavior.

handoff

Resets the session idle timer when MIP user data is detected and an inter-Access Gateway/FA handoff occurs.

normal

Resets the session idle timer when MIP user data is detected and any MIP control signaling occurs.

upstream-only

Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.

Usage Guidelines Use this command to set how the current HA service resets the idle timer for a session.

Example

To reset the idle timer whenever user data is detected or whenever an inter-Access Gateway/FA occurs, use the following command:

idle-timeout-mode handoff

ikev1

Configures IPSec Internet Key Exchange (IKE) parameters.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
ikev1 { aaa-context aaa_context_string | peer-fa  IPAddress crypto-map
crypto_map_string [ encrypted ] [ secret secret_string ] | skew-lifetime seconds
 }
no ikev1 { aaa-context | peer-fa IPAddress | skew-lifetime }
```

no

Disables IPSec IKE parameters.

aaa-context *aaa_context_string*

Configures AAA context from which to retrieve IKE keys. Must be followed by the context name.

aaa_context_string is an alphanumeric string of 1 through 63 characters.

peer-fa *IPAddress*

Sets the IKE crypto-map for a peer Foreign Agent (FA).

IPAddress is IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

crypto-map *crypto_map_string*

Configures IKE crypto-map. Must be followed by the crypto-map name.

crypto_map_string is an alphanumeric string of 1 through 63 characters.

encrypted designates use of encryption

secret *secret_string* uses a secret that is shared between FA and HA. *secret_string* is an alphanumeric string of 1 through 256 characters.

skew-lifetime *seconds*

Configures the "S" lifetime Skew (in seconds). *seconds* is an integer from 1 through 65534. Default is 10.

Usage Guidelines

Use this command to configure IPSec IKE parameters.

Example

```
ikev1 peer-fa 11.22.33.44 crypto-map er encrypted secret ert
```

ip context-name

Specifies name of the destination context to be applied to the subscribers.

This configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context; the IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
ip context-name name
{ default | no } ip context-name
```

default

Sets the default value assigned for context-name.

no

Removes the current assigned context from the subscriber's data.

name

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string from 1 through 79 characters.

Usage Guidelines Set the name of the destination context to be applied to the subscribers.

Example

The following command configures the IP context name of *sampleName*:

```
ip context-name sampleName
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interface's IP socket on which to listen for Mobile IP Registration messages.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
ip local-port number
default ip local-port
```

default

Sets or restores the default value assigned for the IP local port.

number

Specifies the UDP port number.

number is an integer from 1 through 65535. Default is 434.

Usage Guidelines Specify the UDP port that should be used for communications between the FA service and the HA.

Example

The following command specifies a UDP port of *3950* for the HA service to use to communicate with the HA on the Pi interface:

```
ip local-port 3950
```

ip pool

Specifies name of the IP address pool or group to use for subscriber IP address allocation.

This configuration overrides the local subscriber configuration, as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context and an IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

ip pool *name*
{ default | no } ip pool

name

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

no

Removes the specified IP address pool specified from the current context or disables the option for an IP pool.

default

Clears the IP address pool or group setting.

Usage Guidelines

Define a pool of IP addresses for the context to use in assigning IPs for this service.

Example

The specifies name of the IP address pool or group to use for subscriber IP address allocation:

```
ip pool pool1
```

The following command removes the specified IP address pool:

```
no ip pool
```

isakmp

Configures the crypto map for a peer HA and the default crypto map for the FA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
isakmp { peer-fa fa_address |   [ [ encrypted ] secret  ] } | skew-lifetime
 time | aaa-context context_name }
no isakmp { peer-fa fa_address | default | skew-lifetime | aaa-context }
```

no

Deletes the reference to the crypto map for the specified HA; deletes the reference for the default crypto map; resets the skew-lifetime to the default; or resets the aaa-context to the default.

peer-fa *fa_address* { crypto map map_name [[encrypted] secret *secret*] }

Configures a crypto map for a peer FA.

- *fa_address*: IP address of the peer FA to which this IPSec SA will be established.
- **crypto map** *map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is an alphanumeric string of 1 through 63 characters.
- **encrypted**: This keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret** *secret*: The pre-shared secret that will be used to during the IKE negotiation. *secret* is an alphanumeric string of 1 through 127 characters.

skew-lifetime *time*

Default: *10* seconds

Configures the IKE pre-shared key's time skew.

time is the amount of time the fetched from AAA that is considered valid after the key has expired. It is measured in seconds and can be configured to an integer from 1 through 65534.

aaa-context *context_name*

Default: The context in which the service is configured

Configures the name of the context on the system in which AAA functionality is performed.

context_name is the name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters. It is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this command to configure the FA-service's per-HA IPSec parameters. These dictate how the HA service is to establish an IPSec SA with the specified FA.

Important For maximum security, this command be executed for every possible FA with which the HA service communicates.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

Example

The following command creates a reference for an HA with the IP address *10.2.3.4* to a crypto map named *map1*:

```
isakmp peer-fa 10.2.3.4 crypto-map map1
```

The following command deletes the crypto map reference for the HA with the IP address *10.2.3.4*.

```
no isakmp peer-fa 10.2.3.4 crypto-map map1
```

The following command sets the time an S key can used after the S lifetime expires to *120* seconds.

```
isakmp skew-lifetime 120
```

The following command creates the default reference for an HA to a crypto map named *map1*, where peer address is unknown:

```
isakmp default crypto-map map1
```

min-reg-lifetime

Configures Mobile IP session minimum registration lifetime, in seconds.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

[no | default] min-reg-lifetime *min_reg_lifetime_seconds*

no

Disables the min registered lifetime.

default

Configures Mobile IP session minimum registration lifetime to default which is *0*.

min-reg-lifetime

Configures Mobile IP session minimum registration lifetime.

min_reg_lifetime_seconds

This is the minimum registration lifetime value in seconds and must be an integer between 1 through 65534.

Usage Guidelines

Use this command to configure Mobile IP session minimum registration lifetime, in seconds, between *1* and *65534*. Default is *0* seconds.

Example

Use the following command to configure mobile IP session to minimum registered life time to *100* seconds:

```
min-reg-lifetime 100
```

mn-ha-spi

Configures the security parameter index (SPI) between the HA service and the mobile node (MN).

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
mn-ha-spi spi-number number [ description string ] [ encrypted secret
enc_secret ] [ hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } ] [
permit-any-hash-algorithm ] [ replay-protection { nonce | timestamp } ]
[ secret secret ] [ timestamp-tolerance tolerance ]
no mn-ha-spi spi-number number
```

spi-number *number*

Specifies the SPI (number) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. *number* can be configured to an integer from 256 through 4294967295.

description *string*

This is a description for the SPI. *string* is an alphanumeric string of 1 through 31 characters.

encrypted secret *enc_secret* | secret *secret*

Configures the shared-secret between the HA service and the mobile node. The secret can be either encrypted or non-encrypted.

encrypted secret *enc_secret*: Specifies the encrypted shared key between the HA service and the mobile node. *enc_secret* must be an alphanumeric string of 1 through 254 characters that is case sensitive.

secret *secret*: Specifies the shared key between the HA service and the mobile node. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Default: hmac-md5

Specifies the hash-algorithm used between the HA service and the mobile node.

hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.

md5: Configures the hash-algorithm to implement MD5 per RFC 1321.

rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

permit-any-hash-algorithm

Default: disabled

Allows verification of the MN-HA authenticator using all other hash-algorithms after failure with configured hash-algorithm. The successful algorithm is logged to aid in troubleshooting and used to create the MN-HA authenticator in the Registration Reply message.

replay-protection { nonce | timestamp }

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the HA service for this SPI.

nonce: configures replay protection to be implemented using NONCE per RFC 2002.

timestamp: configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance *tolerance*

Default: *60*

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to *0*, timestamp tolerance checking is disabled at the receiving end.

Tolerance is measured in seconds and can be configured to an integer from 0 through 65535.

Usage Guidelines

An SPI is a security mechanism configured and shared by the HA service and the mobile node. Please refer to RFC 2002 for additional information.

Use the **no** version of this command to delete a previously configured SPI.

Example

The following command configures the HA service to use an SPI of 640 when communicating with a mobile node. The key that would be shared between the mobile node and the HA service is q397F65.

```
mn-ha-spi spi-number 640 secret q397F65
```

The following command deletes the configured SPI of *400*:

```
no mn-ha-spi spi-number 400
```

nat-traversal

This command enables NAT traversal and also configures the forcing of UDP tunnels for NAT traversal.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
[ default | no ] nat-traversal [ force-accept ]
```

no

Disables NAT traversal or disables forcing the acceptance of UDP tunnels for NAT traversal.

default

Reset the defaults for this command.

Default: NAT traversal disabled, force-accept disabled.

force-accept

This keyword configures the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request. By default this type of request is rejected if NAT is not detected.

Usage Guidelines

Use this command to enable NAT traversal and enable the forcing of UDP tunnels for NAT traversal.

Example

The following command enables NAT traversal for the current HA service and forces the HA to accept UDP tunnels for NAT traversal:

```
nat-traversal force-accept
```

optimize tunnel-reassembly

Designates that tunnel reassembly optimization will be used for fragmented large packets passed between HA and FA. Default is disabled.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

`[ default | no ] optimize tunnel-reassembly`

Usage Guidelines

Enabling this functionality fragments large packets prior to encapsulation for easier processing.

Tunnel reassembly optimization is disabled by default.

Important You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

Important This functionality works best when the HA service is communicating with an FA service running in a system. However, an HA service running in the system communicating with an FA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the **no** version of this command to disable tunnel optimization if enabled.

Example

The following command enables tunnel reassembly optimization:

`optimize tunnel-reassembly`

per-domain statistics-collection

Enables per-domain statistics collection.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description **`[ no ] per-domain statistics-collection`**

no

Disables per-domain statistics collection.

Usage Guidelines Use this command to enable per-domain statistics collection.

Example

The following command enables per-domain statistics collection.

`per-domain statistics-collection`

policy bc-query-result

Configure the binding cache (BC) query Response Result code.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

`policy bc-query-result network-failure` *`code`*
`default policy bc-query-result network-failure`

network-failure *code*

Default: *0xFFFF*

Specify the response code for BC responses sent on network failures.

code must be either 0xFFFF or 0xFFFE.

Usage Guidelines Use this command to specify the type of response code to send in a P-MIP BC query result.

Example

The following command sets the P-MIP BC query result response code to *0xFFFE*:

```
policy bc-query-result network-failure 0xFFFE
```

policy nw-reachability-fail

Specifies the action to take upon detection of an up-stream network -reachability failure.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
policy nw-reachability-fail { redirect ip_addr1 [ weight value ] [ ip_addr2
[ weight value ] ... ip_addr16 [ weight value ] ] | reject [ use-reject-code
{ admin-prohibited | insufficient-resources } ] }
no policy nw-reachability-fail [ redirect ip_addr1 ... ip_addr16 ]
```

no

Deletes the network reachability policy completely or deletes the specified redirect addresses fro the policy.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

Upon network reachability failure, reject all new calls for this context.

use-reject-code { admin-prohibited | insufficient-resources }: When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

Upon network reachability failure reject all new calls for this context. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

use-reject-code { admin-prohibited | insufficient-resources }: Use the specified reject code when rejecting traffic.

admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

redirect *ip_addr1* [weight *value*] [*ip_addr2* [weight *value*] ... *ip_addr16* [weight *value*]]

Upon network reachability failure redirect all calls to the specified IP address.

ip_addr1: This must entered using IPv4 dotted-decimal notation. Up to 16 IP addresses and optional weight values can be entered on one command line.

weight *value*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified the entry is automatically assigned a weight of 1. *value* must be an integer from 1 through 10.

Usage Guidelines Use this command to set the action for the HA service to take upon a network reachability failure.

Important Refer to the Context Configuration mode command **nw-reachability server** to configure network reachability servers.

Important Refer to the Subscriber Configuration mode command **nw-reachability-server** to bind the network reachability to a specific subscriber.

Important Refer to the **nw-reachability server server_name** keyword of the Context Configuration mode **ip pool** command to bind the network reachability server to an IP pool.

Example

To set the HA service to reject all new calls on a network reachability failure, enter the following command:

policy nw-reachability-fail reject

Use the following command to set the HA service to redirect all calls to the HA at IP address *209.165.200.234* and *209.165.201.10* on a network reachability failure:

```
policy nw-reachability-fail redirect 209.165.200.234 209.165.201.10
```

policy overload

Configures the overload policy within the HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description **policy overload { redirect** *address* **[weight** *weight_num* **] [** *address2* **[weight** *weight_num* **] ... address16 [weight** *weight_num* **]] | reject [use-reject-code {**

```
 admin-prohibited | insufficient-resources } ] }
no policy overload [ redirect address [ address2...address16 ]
```

no policy overload [redirect address [*address2...address16*]]

Deletes a previously set policy or removes a redirect IP address.

overload: Without any options deletes the complete overload policy from the PDSN service.

overload redirect *address* [*address2 ... address16*]: deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted-decimal notation

redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HA service rejects new sessions with a Registration Reply Code of 136H (unknown home agent address) and provides the IP address of an alternate HA. This command can be issued multiple times.

address: The IP address of an alternate HA expressed in IP v4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy, the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

reject [use-reject-code { admin-prohibited | insufficient-resources }]

This option causes any overload traffic to be rejected. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

use-reject-code { admin-prohibited | insufficient-resources }: Use the specified reject code when rejecting traffic.

admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

Usage Guidelines

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the **no** version of this command to restore the default policy.

The setting for overload policy is reject.

Example

The following command enables an overload redirect policy for the HA service that will send overload calls to either of two destinations with weights of *1* and *10* respectively:

```
policy overload redirect 209.165.200.234 weight 1 209.165.200.244 weight
 10
```

policy null-username

Configures the current HA service to accept or reject an RRQ without an NAI extension.



Important This command is customer specific and license enabled.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

```
policy null-username { accept-static | reject }
no policy null-username
```

no

Set the HA back to the default behavior of rejecting an RRQ without an NAI extension.

accept-static

This enable the HA to accept an RRQ with a static (non-zero) home address request but without NAI extension, when MN-AAA authentication is disabled at the HA. MN-NAI is required for MN-AAA authentication.

reject

Default. This is the default behavior of rejecting an RRQ without an NAI extension.

Usage Guidelines

Use this command to enable or disable the HA from accepting an RRQ without an NAI.

Example

The following command enables the current HA service to accept RRQs that do not have an NAI extension:

```
policy null-username accept-static
```

private-address allow-no-reverse-tunnel

This command allows the HA service to accept private addresses without using reverse tunneling.

Important This command is customer specific and license enabled.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description **`[ no ] private-address allow-no-reverse-tunnel`**

no

Reject MIP calls that use private addresses and do not use reverse tunneling.

Usage Guidelines Use this command to enable or disable the HA from accepting calls that use private addresses without reverse tunneling.

Example

The following command enables the current HA service to accept MIP calls that use private addresses but do not use reverse tunneling:

`private-address allow-no-reverse-tunnel`

radius accounting dropped-pkts

This command enables or disables RADIUS accounting related configuration for dropped packets.

Important This command is customer-specific. Contact your Cisco account representative for more information.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
[ no ] radius accounting dropped-pkts
```

no

Enables the RADIUS accounting related configuration for dropped packets.

radius accounting dropped-pkts

Disables the RADIUS accounting related configuration for dropped packets. This is the default behavior.

Usage Guidelines

Use this command to enable or disable the RADIUS accounting related configuration for dropped packets.

By default, the feature is disabled.

Important The configuration will be picked up during **call-setup** and can not be changed dynamically.

Example

The following command enables the RADIUS accounting related configuration for dropped packets for the HA service:

```
no radius accounting dropped-pkts
```

reg-lifetime

Configures Mobile IP session registration lifetime.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
reg-lifetime time
{ default | no } reg-lifetime
```

no

Sets the registration lifetime to infinite.

default

Sets the registration lifetime to default value, 600.

time

Specifies the registration lifetime in seconds.

time is an integer from 1 through 65534.

Usage Guidelines

Use this command o limit a mobile node's lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply. The default is 600 seconds.

Example

The following command configures the registration lifetime for the HA service to be *2400* seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIP calls:

```
no reg-lifetime
```

reverse-tunnel

Enables use of reverse tunneling for Mobile IP session. Use no reverse-tunnel command to disable. If disabled, mobile node (MN) packets are not tunneled to the HA in the reverse direction.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
[ default | no ] reverse-tunnel
```

no

Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

default

Indicates the reverse tunnel option is to be set to the default. When omitted, the reverse tunnel option is enabled.

Usage Guidelines

Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA service via the FA.

When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Among the advantages of using reverse-tunneling are that:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA to which the mobile node is registered and tunnel all datagrams from the mobile node to its HA

Use the **no** version of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, triangular routing will be performed.

Routing will be used.

The default setting is reverse tunnel enabled.



Important If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

Example

The following command disables reverse-tunneling support for the HA service:

```
no reverse-tunnel
```

revocation

Configures the Registration Revocation feature for a specific HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
revocation { enable | max-retransmission number | negotiate-i-bit |
retransmission-timeout secs | send-nai-ext | trigger { handoff |
idle-timeout } }
no revocation { enable | negotiate-i-bit | send-nai-ext | trigger { handoff
 | idle-timeout } }
default revocation [ enable ] [ max-retransmission ] [ negotiate-i-bit ]
 [ retransmission-timeout ] [ send-nai-ext ] [ trigger { handoff |
idle-timeout } ]
```

no

Completely disables registration revocation on the HA, disables trigger handoff, or disables revocation on idle timer expiration.

default

Sets or restores the default value assigned for specified parameter.

enable

Enables the MIP registration revocation feature on the HA. When enabled, if revocation is negotiated with an FA and a MIP binding is terminated, the HA can send a Revocation message to the FA. This feature is disabled by default.

max-retransmission *number*

Default: 3

The maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer from 0 through 10.

negotiate-i-bit

Default: disabled

Enables the HA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout *secs*

Default: 3

The number of seconds to wait for a Revocation Acknowledgement from the FA before retransmitting the Revocation message. *secs* must be an integer from 1 through 10.

send-nai-ext

Default: off

Enables sending the NAI extension in the revocation message.

trigger { handoff | idle-timeout }

handoff: Default: Enabled

Triggers the HA to send a Revocation message to the FA when an inter-Access Gateway/FA handoff of the MIP session occurs. If this is disabled, the HA is never triggered to send a Revocation message.

idle-timeout: Default: Enabled

Triggers the HA to send a Revocation message to the FA when a session idle timer expires.

Usage Guidelines

Use this command to enable or disable the MIP revocation feature on the HA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

Example

The following command enables Registration Revocation on the HA:

revocation enable

The following command sets the maximum number of retries for a Revocation message to *10*:

revocation max-retransmission 10

The following command sets the timeout between retransmissions to *3*:

revocation retransmission-timeout 3

The behavior of send MIP revocation to FA is as follows:

- 1st retry: Retransmit in 3 seconds after previous MIP revocation send.
- 2nd retry: Retransmit in 6 seconds after previous MIP revocation send (9 seconds after sending initial MIP revocation).
- 3rd retry: Retransmit in 12 seconds after previous MIP revocation send (21 seconds after sending initial MIP revocation).
- 4th retry: Retransmit in 24 seconds after previous MIP revocation send (45 seconds after sending initial MIP revocation).
- 5th retry: Retransmit in 48 seconds after previous MIP revocation send (93 seconds after sending initial MIP revocation).



Important The value of retransmission-timeout doubles. HA disconnects the session forcibly in 120 seconds after sending initial MIP revocation.

setup-timeout

The maximum time allowed for session setup in seconds. Default is 60 seconds.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

Syntax Description

setup-timeout *seconds*
default setup-timeout

default

Sets or restores the default value.

seconds

Default: 60 seconds

The maximum amount of time (in seconds) to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

Usage Guidelines Use this command to set the maximum amount of time allowed for setting up a session.

Example

To set the maximum time allowed for setting up a session to 5 minutes (*300* seconds), enter the following command:

```
setup-timeout 300
```

simul-bindings

Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
simul-bindings number
default simul-bindings
```

default

Sets or restores the default value.

number

Configures the maximum number of simultaneous "care-of" bindings that the HA service will maintain for any given subscriber.

is an integer from 1 through 3.

Usage Guidelines

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.

Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintain previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested. The default value is 3.

Example

The following command configures the HA service to support up to 4 MBRs per subscriber:

```
simul-bindings 4
```

threshold dereg-reply-error

Sets an alarm or alert based on the number of de-registration reply errors per HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold dereg-reply-error high_thresh [ clear low_thresh ]
no threshold dereg-reply-error
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of de-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to an integer from 0 through 100000.

clear *low_thresh*

Default: 0

The low threshold number of de-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to an integer from 0 through 100000.

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 high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of de-registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of de-registration reply errors on the following rules:

- **Enter condition:** Actual number of de-registration reply errors > High Threshold
- **Clear condition:** Actual number of de-registration reply errors < Low Threshold

Example

The following command configures a de-registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold dereg-reply-error 1000 clear 500
```

threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0

The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second is greater than the high threshold.
- **Clear condition:** Actual number of calls setup per second is less that the low threshold.

Example

The following command configures a number of calls setup per second threshold of 1000 and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```

threshold ipsec-call-req-rej

Configures a threshold for the total IPSec calls request rejected.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold ipsec-call-req-rej high_thresh [ clear low_thresh ]
no threshold ipsec-call-req-rej
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:*0*

Specifies the low threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IPSec call requests rejected is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE requests is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE requests is less than the low threshold.

Example

The following command configures a number of IPSec call requests rejected threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-call-req-rej 1000 clear 800
```

threshold ipsec-ike-failrate

Configures a threshold for the percentage of IPSec IKE failures.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold ipsec-ike-failrate high_thresh [ clear low_thresh ]
no threshold ipsec-ike-failrate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100.

clear *low_thresh*

Default:*0*

Specifies the low threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the percentage of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the percentage of IPSec IKE failures on the following rules:

- **Enter condition:** Percentage of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Percentage of IPSec IKE failures is less than the low threshold.

Example

The following command configures a percentage of IPSec IKE failures threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failrate 90 clear 80
```

threshold ipsec-ike-failures

Configures a threshold for the total IPSec IKE failures.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

threshold ipsec-ike-failures *high_thresh* **[clear** *low_thresh* **]**
no threshold ipsec-ike-failures

no

Deletes the alert or alarm.

high_thresh

Default: *0*

Specifies the high threshold number of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0

Specifies the low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.

Example

The following command configures a number of IPSec IKE failures threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failures 1000 clear 800
```

threshold ipsec-ike-requests

Configures a threshold for the total IPSec IKE requests.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

threshold ipsec-ike-requests *high_thresh* **[clear** *low_thresh* **]**
no threshold ipsec-ike-requests

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of IPSec IKE requests per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0

Specifies the low threshold number of call IPSec IKE requests per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IPSec IKE requests is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.

Example

The following command configures a number of IPSec IKE requests threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-ike-requests 1000 clear 800
```

threshold ipsec-tunnels-established

Configures a threshold for the total IPSec tunnels established.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

threshold ipsec-tunnels-established *high_thresh* **[clear** *low_thresh* **]**
no threshold ipsec-tunnels-established

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of IPSec tunnels established per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0

Specifies the low threshold number of call IPSec tunnels established per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IPSec tunnels established is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels established on the following rules:

- **Enter condition:** Actual number of IPSec tunnels established is greater than the high threshold.
- **Clear condition:** Actual number of IPSec tunnels established is less than the low threshold.

Example

The following command configures a number of IPSec tunnels established threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-established 1000 clear 800
```

threshold ipsec-tunnels-setup

Configures a threshold for the total IPSec tunnels setup.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold ipsec-tunnels-setup high_thresh [ clear low_thresh ]
no threshold ipsec-tunnels-setup
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of IPSec tunnels setup per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear *low_thresh*

Default:0

Specifies the low threshold number of call IPSec tunnels setup per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.

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 high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of IPSec tunnels setup is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels setup on the following rules:

- **Enter condition:** Actual number of IPSec tunnels setup is greater than the high threshold.
- **Clear condition:** Actual number of IPSec tunnels setup is less than the low threshold.

Example

The following command configures a number of IPSec tunnels setup threshold of *1000* and a low threshold of *800* for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-setup 1000 clear 800
```

threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold reg-reply-error high_thresh [ clear low_thresh ]
no threshold reg-reply-error
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0

Specifies the low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.



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 high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition:** Actual number of registration reply errors is greater than the high threshold.
- **Clear condition:** Actual number of registration reply errors is less than the low threshold.

Example

The following command configures a registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```

threshold rereg-reply-error

Set an alarm or alert based on the number of re-registration reply errors per HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > **context** *context_name* > **ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
threshold rereg-reply-error high_thresh [ clear low_thresh ]
no threshold rereg-reply-error
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of re-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

clear *low_thresh*

Default:0

Specifies the low threshold number of re-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.



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 high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of re-registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of re-registration reply errors on the following rules:

- **Enter condition:** Actual number of re-registration reply errors is greater than the high threshold.
- **Clear condition:** Actual number of re-registration reply errors is less than the low threshold.

Example

The following command configures a reregistration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold rereg-reply-error 1000 clear 500
```

wimax-3gpp2 interworking

Configures the interworking between WiMAX and 3GPP2 network at HA. This support provides handoff capabilities from 4G to 3G (PDSN) network access and vice-versa.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context *context_name* **> ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

Syntax Description

```
[ no | default ] wimax-3gpp2 interworking
```

no

Disables the pre-configured interworking between WiMAX and 3GPP2 networks at HA level.

default

Configures the **WiMAX-3GPP2 interworking** to default setting: disabled.

Usage Guidelines

Use this command to enable/disable the interworking between WiMAX and 3GPP2 network for seamless session continuity.

This functionality provides HA support for both 4G and 3G technology HA (WiMAX HA and PDSN/HA) for handoff from 4G and 3G network access (ASN GW/FA and PDSN/FA) and vice-versa.



Important Use this command in conjunction with the **authentication aaa-distributed-mip-keys required** command.

Example

The following command enables the interworking for a subscriber between WiMAX and 3GPP2 network.

```
wimax-3gpp2 interworking
```