

FA Service Configuration Mode Commands

The Foreign Agent Service Configuration Mode is used to create and manage the Foreign Agent (FA) services associated with the current context.

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

- advertise, on page 2
- authentication aaa, on page 4
- authentication mn-aaa, on page 5
- authentication mn-ha, on page 6
- bind, on page 7
- challenge-window, on page 8
- default subscriber, on page 9
- dynamic-ha-assignment, on page 10
- dynamic-mip-key-update, on page 11
- encapsulation allow gre, on page 12
- end, on page 12
- exit, on page 12
- fa-ha-spi, on page 13
- gre, on page 15
- ha-monitor, on page 17
- idle-timeout-mode, on page 19
- ignore-mip-key-data, on page 19
- ignore-stale-challenge, on page 20
- ip local-port, on page 21
- isakmp, on page 22
- limit-reg-lifetime, on page 23

- max-challenge-len, on page 24
- mn-aaa-removal-indication, on page 25
- multiple-reg, on page 26
- optimize tunnel-reassembly, on page 27
- private-address allow-no-reverse-tunnel, on page 27
- proxy-mip, on page 28
- reg-timeout, on page 30
- reverse-tunnel, on page 31
- revocation, on page 32
- threshold reg-reply-error, on page 33

advertise

Configures agent advertisement parameters within the FA service.

Product

PDSN

GGSN

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
advertise {adv-delay seconds | adv-lifetime time | adv-interval { seconds |
msec num } | num-adv-sent number | prefix-length-extn | reg-lifetime reg_time
 }
no advertise { prefix-length-extn | reg-lifetime }
default advertise adv-delay
```

no

Disables prefix-length-extn.

no advertise reg-lifetime

Specifies that there is no limit to the registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

default advertise adv-delay

Sets the initial delay for the unsolicited advertisement to the default value of 1000 ms.

advertise adv-delay *seconds*

Default: 1000

Sets the initial delay for the unsolicited advertisement.

seconds is the advertisement delay in milliseconds and must be an integer from 10 through 5000.



Important This command is available for WiMAX CMIP calls only.

adv-lifetime *time*

Default: 9000

Specifies the FA agent advertisement lifetime.

The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements.

time is measured in seconds and can be configured to an integer from 1 through 65535.

adv-interval { *seconds* | msec *num* }

Default: 5 seconds

Specifies the amount of time between agent advertisements.

seconds is the time in seconds and can be an integer from 1 through1800.

msec *num*: Configures agent advertisement Interval in milliseconds. *num* can be an integer from 100 through 1800000.

num-adv-sent *number*

Default: 5

Specifies the number of unanswered agent advertisements that the FA service sends upon PPP establishment before rejecting the session.

number can be an integer from 1 through 65535.

prefix-length-extn

Default: Disabled

When enabled, the FA includes the FA-service address in the Router Address field of the Agent Advertisement and appends a Prefix Length Extension in Agent Advertisements with a prefix length of 32.

reg-lifetime *reg_time*

Default: 600

Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

reg_time is measured in seconds and can be configured to an integer from 1 through 65534.

Usage Guidelines

Use to tailor FA advertisements to meet your network needs and/or conditions.

Example

The following command configures the FA advertisement interval at 10 seconds, the advertise lifetime to *20000* seconds, and the maximum number of unanswered advertisements that will be set to *3*.

```
advertise adv-interval 10 adv-lifetime 20000 num-adv-sent 3
```

authentication aaa

This configuration enables or disables the authentication parameters for the FA service to override dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

Product

FA

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] authentication aaa-distributed-mip-keys override
```

no

Disable the override of dynamic keys from AAA.

default

By default the override behavior is disabled and the system uses dynamic keys from AAA after successful EAP authentication. If EAP authentication fails, the system uses static keys by default.

Usage Guidelines

Specify how the system will perform authentication of registration request messages. By default dynamic MN-HA and FA-HA keys from AAA after successful EAP authentication used by a PMIP client in WiMAX calls for MIP registration with HA. This configuration in FA service overrides the dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

Example

The following command configures the FA service to override use of AAA MIP keys and force the use of statically configured FA-HA SPI/key for WiMAX calls.

```
authentication aaa-distributed-mip-keys override
```

authentication mn-aaa

Specifies how the system handles authentication for mobile node re-registrations.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

authentication mn-aaa { always | ignore-after-handoff | init-reg | init-reg-except-handoff | renew-and-dereg-noauth | renew-reg-noauth } [optimize-retries]

always

Specifies that the FA service performs authentication each time a mobile node registers. This is the default setting.

ignore-after-handoff

MN-AAA authentication is not done at the FA for a handoff Access Gateway (AGW).

init-reg

MN-AAA and MN-FAC extensions are required only in initialization RRQ.

init-reg-except-handoff

MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-Access Gateway (AGW) handoff.

renew-and-dereg-noauth

Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.

renew-reg-noauth

Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration are handled normally.

optimize-retries

Optimizes the number of Authentication retries sent to the AAA server.

When an authentication request is pending for a MIP call at the AGW, if a retry RRQ is received from the mobile node, the AGW discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the AGW forwards the most recent RRQ to the HA. If the authentication fails, the AGW replies to the MN using the most recent RRQ.

Usage Guidelines

Use this command to determine how the FA service handles mobile node re-registrations.

The system is shipped from the factory with the mobile AAA authentication set to always.

Example

The following command configures the configures the FA service to perform mobile node authentication for every re-registration:

```
authentication mn-aaa always
```

The following command specifies that the FA service does not perform authentication for mobile node re-registrations:

```
authentication mn-aaa renew-reg-noauth
```

authentication mn-ha

Configures whether the FA service looks for a Mobile Network-Home Agent (MN-HA) authentication extension in the RRP (registration reply).

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
authentication mn-ha { allow-noauth | always }
```

allow-noauth

Allows a reply that does not contain the auth extension.

always

A reply should always contain the auth extension to be accepted.

This is the default setting.

Usage Guidelines

Use this command to determine whether or not the FA service requires the MN-HA auth extension in the RRP.

The system is shipped from the factory with this set to always.

Example

The following command configures the FA service to require a reply to contain the authentication extension to be accepted.:

```
authentication mn-ha always
```

bind

Binds the FA 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

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bind address address [ max-subscribers count ]
no bind address
```

address

Specifies the IP address (address) of the interface configured as the Pi interface. *address* is specified in IPv4 dotted-decimal notation.

max-subscribers *max#*

Default: 500000

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

count can be configured to an integer from 0 through 500000.

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. Refer to the license key command for additional information.

Usage Guidelines

Associate or tie the FA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an 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 you will configure 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 (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

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.

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 *209.165.200.224* to the FA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 209.165.200.224 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

challenge-window

Defines the number of recently sent challenge values that are considered valid by the FA.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

challenge-window *number*

number

Default: 2

The number of recently sent challenge values that are considered valid. *number* must be an integer from 1 through 5.

Usage Guidelines

Use this command to set the number of recently sent challenge values that are considered valid by the FA.

Example

Set the challenge window to *3*:

challenge-window 3

default subscriber

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

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-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 63 characters that is case sensitive.

Usage Guidelines

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

By default, the FA service will use the information configured for the subscriber named default within the same context. This command allows for multiple FA 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 FA 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
```

dynamic-ha-assignment

This command configures various dynamic HA assignment parameters.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] dynamic-ha-assignment [ aaa-override mn-supplied-ha-addr
 | allow-failover ]
```

default

Feature is disabled by default.

no

Removes the feature and returns it to the default setting of disabled.

aaa-override mn-supplied-ha-addr

Enables the system to override the mobile node supplied HA IP address with the AAA provided HA address.

allow-failover

Enables/disables a failover retry for dynamic HA assignment from the AAA server.

Usage Guidelines

Use this command to override the mobile node supplied HA IP address with the AAA supplied HA address.

Use this command to enable or disable the failover feature that allows the system to receive and use a newer HA address from the AAA server in cases where the original HA address is not responding.

A AAA server may assign different HA addresses each time a retransmitted MIP RRQ is authenticated during the MIP session setup. When this configuration is enabled, if the FA gets a new HA address from AAA during setup, it discards the previous HA address and start using the new address. This allows the FA session to connect to an available HA during setup.

Example

The following command enables the failover feature that allows the system to receive and use a newer HA address from the AAA server:

```
dynamic-ha-assignment allow-failover
```

dynamic-mip-key-update

When enabled, the FA service processes MIP_Key_Update_Request from the AAA server and allows dynamic MIP key updates (DMUs).

Default: Disabled

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] dynamic-mip-key-update

no

The FA service rejects MIP_Key_Update_Request from the AAA server, not allowing dynamic MIP key updating to occur and terminates the call.

Usage Guidelines

Use this command to enable or disable the DMU feature in the FA service.

Example

To enable DMU and allow dynamic updates of MIP keys, enter the following command:

```
dynamic-mip-key-update
```

encapsulation allow gre

Enables or disables the use of generic routing encapsulation (GRE) when establishing a Mobile IP (MIP) session. When enabled, if requested by a Mobile Node (MN), the FA requests the HA to use GRE encapsulation when establishing the MIP session. When disabled, the FA does not set the GRE bit in Agent Advertisements to the MN.

Default: GRE is enabled.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] encapsulation allow gre`

Usage Guidelines

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

Example

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

`encapsulation allow 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) between the FA service and the HA.

Product PDSN

ASN-GW

GGSN

PDIF

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number
 { encrypted secret enc_secret | secret } [ description string |
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | monitor-ha |
replay-protection { timestamp | nonce } | timestamp-tolerance tolerance ]
 no fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number
number
```

remote-address { *ha_ip_address* | *ip_addr_mask_combo* }

ha_ip_address: Specifies the IP address of the HA in IPv4 dotted-decimal notation.

ip_addr_mask_combo: Specifies the IP address of the HA including network mask bits. *ip_addr_mask_combo* must be specified IPv4 dotted-decimal notation with CIDR subnet mask bits (x.x.x.x/xx).

spi-number *number*

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

number can be configured to an integer from 256 through 4294967295.

encrypted secret *enc_secret* | secret *secret*

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

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



Important The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **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*: Specifies the shared key (secret) between the FA service and the HA. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

description *string*

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

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

Default: hmac-md5

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

- **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.

monitor-ha

Default: disabled

Enables the HA monitor feature for this HA address.

To set the behavior of the HA monitor feature, refer to the **ha-monitor** command in this chapter. To disable this command (if enabled) for this HA address, re-enter the entire **fa-ha-spi** command without the **monitor-ha** keyword.

replay-protection { timestamp | nonce }

Default: timestamp

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. Nonce is an arbitrary number used only once to sign a cryptographic communication.
- **timestamp**: Configures replay protection to be implemented using timestamps per RFC 2002.



Important This keyword should only be used in conjunction with Proxy Mobile IP support.

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, then timestamp tolerance checking is disabled at the receiving end.

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



Important This keyword should only be used in conjunction with Proxy Mobile IP support.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

An SPI is a security mechanism configured and shared by the FA service and the HA. 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 FA 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 *209.165.200.224*. 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 209.165.200.224 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 *209.165.201.0*:

```
no fa-ha-spi remote-address 209.165.201.0 spi-number 400
```

gre

Configures Generic Routing Encapsulation (GRE) parameters.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Disables the specified functionality.

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 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 insertion or removal of GRE sequence numbers in GRE packets.

Usage Guidelines Use this command to configure how the FA service handles GRE packets.

Example

To set 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
```

ha-monitor

Configures the behavior of the HA monitor feature.

Product PDSN

ASN-GW

FA

HA

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default ] ha-monitor [ interval sec | max-inactivity-time sec | num-retry num ]
no ha-monitor
```

default

Restores the system default setting(s) for the command/keyword(s). This command is disabled by default.

no

Disables the HA monitoring feature for this FA service.

interval *sec*

Default: 30

Configures the time interval before the next monitoring request message is sent to the HA.

sec must be an integer from 1 through 36000.

max-inactivity-time *sec*

Default: 60

Specifies the maximum amount of time the system will wait without receiving MIP control traffic from a HA before the HA monitoring mechanism is triggered.

sec must be an integer from 30 through 600.

num-retry *num*

Default: 5

Configures the number of time the system will attempt to send HA monitor requests before determining the HA is down and a trap is initiated.

num must be an integer from 0 through 10.

Usage Guidelines

Use this command to set parameters for the HA monitor feature. This feature allows the AGW/FA to monitor HAs with which it has MIP sessions. The monitoring feature is triggered when the AGW/FA does not receive any MIP traffic from a HA for a configured amount of time (**max-inactivity-time**). The AGW/FA starts sending special MIP RRQ monitor messages and waits for RRP monitor message responses from the HA. The RRQ monitor messages are addressed to the HA service address. The source address of the monitor-request messages is the FA service's IP address.

The actions taken during monitoring are comprised of the following:

- If no monitor response is received during the interval time (**interval**), the AGW retransmits the monitor message a configured number of times (**num-retry**).
- If no response is received after retransmitting for the number configured in **num-retry**, the HA is considered down. The AGW/FA sends a trap (HAUnreachable) to the management station. Monitoring of this HA is stopped until a MIP control message is received from the particular HA and when the AGW/FA sends a trap (HAreachable) to the management station and starts monitoring the HA again.
- When an HA receives the RRQ from an FA, it verifies the message and identifies it as a monitor message based on a special reserved NAI (in the message) and a Monitor HA CVSE in the RRQ. The HA responds with an RRP with Reply code 0x00 (accepted) and includes the Monitor HA CVSE. When the FA receives the RRP from the HA, it updates the activity for the peer HA to maintain the "up" state.



Important This command only sets the behavior of the HA monitor feature. To enable the HA monitor feature for each HA address, refer to the **fa-ha-spi** command in this chapter. Up to 256 HAs can be monitored per system.

Example

The following commands set the HA monitor message interval to *45* seconds, the HA inactivity time to *60* seconds, and the number of HA monitor retries to *6*:

```
ha-monitor interval 45
ha-monitor max-inactivity-time 60
ha-monitor num-retry 6
```

idle-timeout-mode

Controls whether Mobile IP data and control packets or only Mobile IP data resets the session idle timer.

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`idle-timeout-mode { aggressive | normal }`

aggressive

Only Mobile IP data resets the session idle timer.

normal

Both Mobile IP data and control packets reset the session idle timer.

Usage Guidelines

Use this command to control how the session idle timer is reset.

Example

The following command specifies that only Mobile IP data can reset the session idle timer:

`idle-timeout-mode aggressive`

ignore-mip-key-data

When this command is enabled, if the Dynamic Mobile IP Key Update (DMU) is not enabled and the mobile node (MN) sends a MIP_Key_Data CVSE, the FA ignores the MIP_Key_Data extension and the call is continued like a regular Mobile IP (MIP) call.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] ignore-mip-key-data`

no

Disable ignoring of MIP key data.

Usage Guidelines

When DMU is not enabled, use this command to ignore MIP key data sent by the MN and allow the call to continue normally.

Example

To enable the FA to ignore MIP key data sent by the MN, enter the following command:

`ignore-mip-key-data`

ignore-stale-challenge

Enables the system to accept RRQs with previously used challenges. This feature is disabled by default.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] ignore-stale-challenge`

no

Disables this feature. If an RRQ is received with a previously used challenge and there are RRQs pending on the same session, accept the RRQ if it has a new Identification in the retransmitted RRQ. All other RRQs received with previously used challenge are rejected with the Stale Challenge (106) error code.

Usage Guidelines

Use this command to allow the FA to accept stale challenges regardless of the ID field or if other RRQs are pending.

Example

To enable this functionality in the FA service, enter the following command;

```
ignore-stale-challenge
```

To disable this functionality, enter the following command;

```
no ignore-stale-challenge
```

ip local-port

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

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip local-port *port#*

port#

Specifies the UDP port number.

port# can be an integer from 1 through 65535.

Usage Guidelines

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

The system defaults to using local port 434.

Example

The following command specifies a UDP port of *3950* for FA-to-HA communication on the Pi interface:

```
ip local-port 3950
```

isakmp

Configures support for IPSec within the FA-service.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

isakmp {peer-ha *ha_address* **{ crypto map** *map_name* **[[encrypted] secret** *secret* **] } | default { crypto map** *map_name* **[[encrypted] secret** *secret* **] } }**
no isakmp { peer-ha *peer_ip_address* **| default }**

no

Deletes the reference to the crypto map for the specified HA, or deletes the reference for the default crypto map.

peer-ha *ha_address* { crypto map *map_name* [[encrypted] secret *preshared_secret*] }

Configures a crypto map for a peer HA.

- *ha_address*: The IP address of the HA with which the FA service will establish an IPSec SA. The address must be expressed in IPv4 dotted-decimal format.
- **crypto map** *map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.
- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **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 during the IKE negotiation. *preshared_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

default { crypto map *map_name* [[encrypted] secret *secret*] }

Specifies the default crypto map to use when there is no matching crypto map configured for an HA address.

- **crypto map** *map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.

- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **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 during the IKE negotiation. *preshared_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

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



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

A default crypto map can also be configured using the default keyword. The default crypto map is used in the event that the AAA server returns an HA address that is not configured as an isakmp peer-ha.



Important For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs.

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 *209.165.200.229* to a crypto map named *map1*:

```
isakmp peer-ha 209.165.200.229 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address *209.165.200.229*.

```
no isakmp peer-ha 209.165.200.229
```

limit-reg-lifetime

Enable the current default behavior of limiting the Mobile IP (MIP) lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts. When disabled, this command allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] limit-reg-lifetime

no

Allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

default

Enables the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Usage Guidelines

Use the no keyword with this command to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Use the base command or the keyword to reset the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Example

Configure the FA service to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts by entering the following command:

no limit-reg-lifetime

Configure the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts by entering either of the following commands:

```
default limit-reg-lifetime
limit-reg-lifetime
```

max-challenge-len

For mobile subscribers, the FA generates a random number and sends it to the mobile node as part of the mobile authentication extension (Mobile-Foreign Authentication extension) as described in RFC 3012. This command sets the maximum length of the FA challenge in bytes.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-challenge-len *length*

length

Default: 16

The maximum length, in bytes, of the FA challenge. This value must be an integer from 4 through 32.

Usage Guidelines

Change the maximum allowed length of the randomly generated FA challenge its default of 16.

Example

Use the following command to change the maximum length of the FA challenge to 18 bytes:

max-challenge-len 18

mn-aaa-removal-indication

Enables the FA to remove the Mobile Network-Final Assembly Code (MN-FAC) and MN-AAA extensions from RRQs. This is disabled by default.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] mn-aaa-removal-indication

no

Disable the removal of the MN-FAC and MN-AAA extensions from RRQs.

Usage Guidelines

Enable this feature if there is no need to authenticate the subscriber at HA using MN-AAA extension.

Example

The following command enables the FA service to remove MN-FAC and MN-AAA extensions from RRQs:

mn-aaa-removal-indication

multiple-reg

Specifies the number of simultaneous Mobile IP sessions that will be supported for over a single PPP session.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

multiple-reg *number*

number

number can be configured to an integer from 1 through 3.

Usage Guidelines

Use to support multiple registrations per subscriber.

The system defaults to a setting of "1" for multiple simultaneous MIP sessions.



Important The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address. The system will only allow a single Mobile IP session for mobile nodes that receive a dynamically assigned IP address. In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

Example

The following command configures the number of supported simultaneous registrations for subscribers using this FA service to *3*.

multiple-reg 3

optimize tunnel-reassembly

Configures FA to HA optimization for tunnel reassembly.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ 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 FA service is communicating with an HA service running in a system. However, an FA service running in the system communicating with an HA 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 it was previously enabled.

Example

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```

private-address allow-no-reverse-tunnel

This command enables the FA to allow calls with private addresses and no reverse tunneling.

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] private-address allow-no-reverse-tunnel

no

Disables the functionality. This is the default setting.

Usage Guidelines

Use this command to let the FA allow sessions with private addresses that do not have the reverse tunnel bit set.

Example

To enable sessions with private addresses and no reverse tunneling, enter the following command:

private-address allow-no-reverse-tunnel

proxy-mip

Configures parameters pertaining to Proxy Mobile IP support.

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

proxy-mip { allow | ha-failover [max-attempts *max_attempts* **|**
num-attempts-before-switching *num_attempts* **| timeout seconds]|**
max-retransmissions number | renew-percent-time *renew-time* **|**
retransmission-timeout *time* **}**

```
no proxy-mip {allow | ha-failover }
default proxy-mip { allow | ha-failover | max-retransmissions |
renew-percent-time | retransmission-timeout }
```

no

Disables FA service support for Proxy Mobile IP or HA failover for Proxy Mobile IP.

default

Restores the specified option to the default setting as described below.

allow

Default: Disabled

Enables FA service support for Proxy Mobile IP.

ha-failover [max-attempts *max_attempts* | num-attempts-before-switching *num_attempts* | timeout *seconds*]

Default: Disabled

Enables HA failover for the Proxy Mobile IP feature.

- **max-attempts** *max_attempts* - Configures the maximum number of retransmissions of Proxy MIP control messages. *max_attempts* must be an integer from 1 through 10. Default is 4
- **num-attempts-before-switching** *num_attempts* - Configures the total number of RRQ attempts (including retransmissions) before failing over to the alternate HA. *num_attempts* must be an integer from 1 through 5. Default is 2.
- **timeout** *seconds* - Configures the retransmission timeout (in seconds) of Proxy MIP control messages when failover happens. *seconds* must be an integer from 1 through 50. Default is 2

max-retransmissions *number*

Default: 5

Configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.

number is the maximum number of retries and can be configured to an integer from 1 through 4294967295.

renew-percent-time *renew-time*

Default: 75

Configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

renew-time is entered as a percentage of the advertisement registration lifetime configured for the FA service. (Refer to the **advertise** command in this chapter). *renew-time* can be configured to an integer from 1 through 100.

The following equation can be used to calculate *renew-time*:

renew-time = (duration / lifetime) * 100

duration = The desired amount of time that can pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request

lifetime = The advertisement registration lifetime configured for the FA service.

duration / lifetime

retransmission-timeout *time*

Default: 3

Configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.

time is measured in seconds and can be configured to an integer from 1 through 100.

Usage Guidelines

The **proxy-mip** command and its keywords configure the FA services support for Proxy Mobile IP.

When enabled though the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

In addition to the parameters configured via this command, the HA-FA SPI(s) must also be modified to support Proxy Mobile IP. Refer to the **fa-ha-spi** command for more information.

Example

The following command configures the FA service to wait up to *5* seconds for an HA to respond prior to re-sending an a Mobile IP Registration Request message:

```
proxy-mip retransmission-timeout 5
```

If the advertisement registration lifetime configured for the FA service is 900 seconds and you want the system to send a Proxy Mobile IP Registration Renewal Request message after 500 seconds, then the following command must be executed:

```
proxy-mip renew-percent-time 50
```

Note that 50 = (450 / 900) 100.

reg-timeout

Configures the FA registration reply timeout.

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

reg-timeout *time*

time

Default: 45

time is measured in seconds and can be configured to an integer from 1 through 65535.

Usage Guidelines

Configure the amount of time that the FA service will wait for a Registration Reply from an HA before the call is rejected with a reply code of 78H (registration Timeout).

Example

The following command configures a registration timeout of 10.

```
reg-timeout 10
```

reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP (MIP) sessions when requested by the mobile node (MN).

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] reverse-tunnel

no

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

Usage Guidelines

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

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.

The advantages of using reverse-tunneling:

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

Use the **no** option of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, then triangular routing is used.

The system defaults to reverse tunnel enabled.



Important If reverse tunneling is disabled on the system and an MN 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 FA service:

```
no reverse-tunnel
```

revocation

Enables the MIP revocation feature and configures revocation parameters.

Product

PDSN

ASN-GW

GGSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
revocation { enable | max-retransmission number | negotiate-i-bit |
retransmission-timeout secs | trigger internal-failure }
no revocation enable | trigger internal-failure | negotiate-i-bit
```

no

Completely disables registration revocation on the FA.

Disables sending revocation messages to the HA when a session is affected by an internal task failure.

enable

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

max-retransmission *number*

Default: 3

Specifies 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 FA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout *secs*

Default: 3

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

trigger internal-failure

Default: disabled

Enable sending a revocation message to the HA for all sessions that are affected by an internal task failure.

Usage Guidelines

Use this command to enable or disable the MIP revocation feature on the FA 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 FA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```

threshold reg-reply-error

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

Product

PDSN

ASN-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-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

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* can be an integer from 0 through 100000.

Important You must enter a value between 1 and 100000 to trigger an alert/alarm.

clear *low_thresh*

Default:0

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* can be 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.

Important You must enter a value between 1 and 100000 to trigger an alert/alarm.

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 > High Threshold
- **Clear condition**: Actual number of registration reply errors £ 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
```