Service Configuration Procedures

This chapter is intended to be used in conjunction with the previous chapters that provide examples for configuring the system to support Simple IP services, Mobile IP services, or both. It provides procedures for configuring the various elements to support these services.

It is recommended that you first select the configuration example that best meets your service model, and then use the procedures in this chapter to configure the required elements for that model.

Note At least one packet processing card must be made active prior to service configuration. Information and instructions for configuring packet processing cards can be found in the "Configuring System Settings" chapter of the *System Administration Guide*.

Procedure are provided for the following:

Creating and Configuring HA Services

HA services are configured within contexts and allow the system to function as an HA in the 3G wireless data network.

To create and configure an HA service:

Step 1 Create and configure an HA service as described in the Creating and Configuring an HA Service, on page 2 section.

Step 2 Verify your configuration as described in the Verifying HA Service Configuration, on page 2 section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in the MIP Timer Considerations appendix.

Creating and Configuring an HA Service

Use the following example to configure HA services:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 ip local-port <port_number>
 authentication mn-aaa { allow-noauth | always | dereg-noauth | noauth |
 renew-and-dereg-noauth | renew-reg-noauth }
 fa-ha-spi remote-address <fa_ip_address> spi-number <number> { encrypted secret
 <enc_secret> | secret <secret> } [ description <string> ] [ hash-algorithm {
hmac-md5 | md5 | rfc2002-md5 } ]
               mn-ha-spi spi-number <number> [ description <string> ] {
encrypted secret <enc_secret> | secret <secret> } [ hash-algorithm { hmac-md5
 | md5 | rfc2002-md5 } ] [ permit-any-hash-algorithm ] [ replay-protection
 { nonce | timestamp } [ timestamp-tolerance <tolerance> ]
 reg-lifetime <lifetime>
 simul-bindings <simul_bindings>
 bind address <address> max-subscribers <max_subs>
 end
```

Notes:

- <*port_number*> must be the UDP port for the Pi interfaces\' IP socket.
- A maximum of 2048 FA-HA Security Parameter Index (SPI) can be configured for each HA service.
- <*lifetime*> must the longest registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured using the **no reg-lifetime** command.
- Option: To configure the HA service for controlling the negotiation and sending of the I-bit in revocation messages, in the HA Service Configuration Mode, enter the following comand. By default, HA will not send I-bit in revocation message. **revocation negotiate-i-bit**
- Use the bind address command to bind the service to the Pi interface and specify the maximum number of subscribers that can access the service. The hardware configuration and features installed can affect the maximum subscriber sessions that can be supported.
- Option: To set the maximum period of time to set up a session, in the HA Service Configuration Mode, enter the following command: **setup-timeout** <*seconds*>
- Create and bind additional HA services to any other interfaces as required.

Verifying HA Service Configuration

Verify that your HA services were created and configured properly by entering the following command:

show ha-service { name service_name | all }

The output is a concise listing of HA service parameter settings similar to the following sample. In this sample, an HA service named ha1 was configured.

```
Service name:  ha1
  Context: ha
  Bind:                Done               Max Subscribers: 500000
  Local IP Address:    192.168.4.10 Local IP Port:   434
  Lifetime:            00h01m40s          Simul Bindings:  3
  Reverse Tunnel:      Enabled
  GRE Encapsulation with-key: Enabled   Keyless GRE Encapsulation: Disabled
  Optimize Tunnel Reassembly: Enabled    Setup Timeout:   60 sec
  Allow Priv Addr w/o Rev Tunnel: Disabled
  WIMAX-3GPP2 Interworking: Disabled
  SPI(s):
  MNHA: Remote Addr: 0.0.0.0             Description:
    Hash Algorithm:    HMAC_MD5          SPI Num:  258
    Replay Protection: Nonce             Timestamp Tolerance: 100
    Permit Any Hash Algorithm:    Enabled
  FAHA: Remote Addr: 195.20.20.6/32 Description:
    Hash Algorithm:    HMAC_MD5          SPI Num:  258
    Replay Protection: Timestamp         Timestamp Tolerance: 60
  'S' Lifetime Skew:   00h00m10s
  IPSEC AAA Context: aaa_context
  GRE Sequence Numbers: Disabled         GRE Sequence Mode: None
  GRE Reorder Timeout:  100 msec
  GRE Checksum:         Disabled         GRE Checksum Verification: Disabled
  Registration Revocation:    Disabled    Reg-Revocation I Bit: Enabled
  Reg-Revocation Max Retries: 3           Reg-Revocation Timeout: 3 (secs)
  Reg-Rev Handoff old-FA:     Enabled     Reg-Rev Idle-Timeout: Enabled
  Send NAI Extension in Reg-Revocation: Disabled
  MIP NAT Traversal: Disabled    Force UDP Tunnel: Enabled
  Default Subscriber:      None
  Max Sessions: 500000
  Service Status: Started
  MN-AAA Auth Policy:      Always
  MN-HA Auth Policy:       Always
  IMSI Auth:               Disabled
  DMU Refresh Key:         Disabled
  AAA Distributed MIP Keys:Disabled
  AAA accounting:          Enabled
  Idle Timeout Mode:       Aggressive
  Newcall Policy:          None
  Overload Policy:         Reject    (Reject code: Admin Prohibited)
  NW-Reachability Policy:  Reject    (Reject code: Admin Prohibited)
  Null-username Policy:    Reject
  BC Rsp Code for Nw Fail: 0xffff
  IP Pool/Group:
    Name: n/a
    Destination Context: n/a
```

Session Continuity Support

This section describes the procedure to enable the mobility for WiMAX subscriber and other access technology subscribers; i.e. 3GPP2. WiMAX HA implementation differs from 3GPP2 on the keys used to authenticate MN-HA and FA-HA AE in MIP RRQ. WiMAX HA involves using dynamic keys distributed by AAA for authenticating RRQ.

Following WiMAX support is provided for MIP keys management and WiMAX HA support:

- MIPv4 support
- Managing MIP Key distribution from AAA
- Registration Revocation
- MIPv4 RRQ with NAI extension
- Support of GRE key extension of CVSE in RRP
- MIPv4 Registration

For MIP registration HA uses the following extensions:

- MN-NAI Extension
- MN-HA AE
- Revocation Support Extension
- FA-HA AE

The MIP client includes the same NAI in all MIP RRQs it sends for the entire duration of the MIP session regardless of EAP re-authentication, including MIP renewal and de-registration messages. The MN-HA and FA-HA keys based on WiMAX VSA from AAA is used to authenticate the RRQ and compute authenticator in RRP.

Authentication algorithm used to authenticate MN-HA and FA-HA AE is HMAC-MD5. If renew/dereg RRQ is received, authentication with AAA will happen only if SPI value for authentication extension in RRQ changes. If SPI returned by AAA is different from the requested one, the RRQ will be rejected. Both MN-HA and FA-HA AE are expected in MIP RRQ for WiMAX calls.

The following describes the processing of different requests for HA support:

- Processing Access-Request: When initial MIP RRQ is received, HA authenticates with AAA to get the MIP Keys (MN-HA and HA-RK) required to authenticate MIP RRQ.
- Processing Access-Accept: In the Access Accept, MIP Keys MN-HA and HA-RK (if requested) is received. MN-HA key is maintained for each subscriber session and FA-HA key is computed based on HA-RK maintained per HA.

All the attributes (HA-RK-KEY, HA-RK-SPI, and HA-RK-Lifetime) must be returned if HA-RK key is requested for the HA-RK info in Access Accept to be valid.

Message Authenticator will be included in Access request and Accept packets for integrity protection of RADIUS packets and is mandatory.

- MIPv4 Revocation: MIP Revocation is supported as per RFC 3543 and it uses FA-HA keys fetched dynamically from AAA during MIP registration.

Apart from these processing, HA provides following function applicable to WiMAX HA.

- Functional Level Description: HA retrieves the MIP Keys dynamically from AAA to authenticate the RRQ.
- Authentication of MIP RRQ in WiMAX HA: When a MIP RRQ is received HA authenticates the user with AAA for both P-MIP and C-MIP call to get the MIP Keys.

The MN-HA and FA-HA keys will be used to authenticate the RRQ.

Hybrid HA Service Configuration

With this support an HA can work in a "hybrid" mode, meaning the same HA can handle a call from CDMA network, a call from WIMAX network, and a "hybrid call" with RRQ coming from one network and later from another network. This way, the operator can just deploy one HA service to support both types of network, instead of using two separate HA services. The HA is aware of the access technology, and choose the correct authentication method to handle RRQ.

This section describes the following configuration procedures:

- Configuring WiMAX HA for WiMAX Calls only, on page 5
- Configuring WiMAX HA to Accept 3GPP2/Static MIP Key, on page 6
- Configuring Hybrid HA for WiMAX and 3GPP2 Calls, on page 6

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring WiMAX HA for WiMAX Calls only

With this configuration the system will support only WiMAX HA behavior for the particular HA-service, where the system always expects WiMAX MIP keys from AAA and use it to do MN-HA and FA-HA authentication extension. With this configuration HA cannot support calls with static keys for MIP RRQ authentication in the particular HA service.

To configure WiMAX HA for WiMAX calls only:

Step 1 Configure WiMAX HA for WiMAX calls only as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to configure WiMAX HA services, and enable the usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with keys mandatory.

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys required
 end
```

Configuring WiMAX HA to Accept 3GPP2/Static MIP Key

To configure WiMAX HA to accept 3GPP2/Static MIP key:

Step 1 Configure WiMAX HA to accept 3GPP2/Static MIP key as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to configure HA services to accept 3GPP2 calls and disable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ.

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys disabled
 end
```

Configuring Hybrid HA for WiMAX and 3GPP2 Calls

With this configuration, both WiMAX and 3GPP2 based calls can be made where WiMAX based calls will use WiMAX MIP keys, and 3GPP2 calls can use static or 3GPP2 based dynamic keys. This particular HA service configuration supports calls of both access technologies.

To configure Hybrid HA for WiMAX and 3GPP2 calls:

Step 1 Configure Hybrid HA to accept WiMAX and 3GPP2 calls in the same service as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to configure HA services to accept WiMAX and 3GPP2 calls in the same service, and enable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with fallback option to use 3GPP2/static keys:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys optional
 wimax-3gpp2 interworking
 end
```

WiMAX-3GPP2 Interworking at HA

The session continuity capability enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective.

This capability provides the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity

To provide this capability, the HA supports seamless handoff from 3GPP2 to WIMAX and vice versa.

This section describes the key configuration to enable this capability.

Mobile Node Requirement

Following are the mandatory functional requirements on mobile node to support 3GPP2-WIMAX Interworking at HA:

- The dual mode MS SHOULD use PMIP to access WIMIAX network and use CMIP to access 3GPP2 network.
- The static NAI (the NAI that is pre-provisioned for access to 3GPP2) has to be used in RRQ on both 3GPP2 and WiMAX networks.
- The dual mode MS SHOULD support "make-before-break" when changing between 3GPP2 and WiMAX networks, if coverage is available on both networks.
- The CMIP4 RRQ message used on 3GPP2 network MUST contain the MN-AAA and Foreign Agent Challenge Extension (FACE)

H-AAA Requirements

H-AAA MUST meets the following requirements to support 3GPP2-WIMAX Interworking at HA:

- The H-AAA servers used by 3GPP2 and WIMAX SHOULD be either the same or they have access to the same session state and subscriber profile.
- H-AAA server SHOULD assign and return the same HA address in response to 3GPP2 and WIMAX network access request

FA and HA Function for 3GPP-WiMAX Interworking at HA

The FA and PMIP4 client provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- For WiMAX access, the PMIP4 Client will NOT include MN-AAA AE in the RRQ.

- For 3GPP2 access, the FA will NOT remove the MN-AAA AE from the RRQ. This requirement stands even if the cdma2000 AAA sends the MN-AAA Removal Indication VSA with its value set.

The HA provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- The HA recognizes the difference between 3GPP2 and WiMAX access technologies based on the presence or absence of MN-FA and MN-AAA AE. If the MN-FA and MN-AAA are present in the RRQ, the HA assumes that the RRQ is coming through a 3GPP2 network. Otherwise, the HA assumes that the RRQ is coming through a WiMAX network.
- The HA updates mobility bindings for different access technology types while maintaining binding integrity (binding continues to be active until updated).
- The same HA is able to handle packets from the MS with a given Care-of Address when the mobility binding is pointing to a different Care-of Address. This is to mitigate packet loss in the uplink during seamless mobility across access technologies.

Before configuring the 3GPP-WiMAX Interworking the following must be taken into consideration:

- Separate FA service is used for 3GPP2 and WIMAX network.
- The subscriber MUST be authorized to use PMIP for WIMAX access.
- The subscriber MUST use CMIP to access 3GPP2 network and MUST NOT set s-bit in RRQ.

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring WiMAX FA Service

To configure WiMAX FA service:

Step 1 Configure WiMAX FA service as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to configure WiMAX FA service:

```
configure
  <context_name>
context
 fa-service <fa_service_name>
 authentication aaa-distributed-mip-keys override
 revocation negotiate-i-bit
 end
```

Configuring 3GPP2 FA Service

To configure 3GPP2 FA service:

Step 1 Configure 3GPP2 FA service as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to create and configure 3GPP2 FA service:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 default mn-aaa-removal-indication
 revocation negotiate-i-bit
 end
```

Important Notes:<*fa_service_name*> must be the FA service designated for 3GPP2 service.

Configuring Common HA Service

To configure common HA service:

Step 1 Configure common HA service as described in this section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Use the following example to configure common HA service:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys required
 wimax-3gpp2 interworking
 authentication mn-aaa allow-noauth
 revocation negotiate-i-bit
 end
```