CHAPTER 16

Other Configuration Tasks

Other Configuration Tasks

This chapter discusses important concepts and provides configuration details for the following features in the Cisco IOS Mobile Wireless Home Agent software:

HA - Realm Case-Insensitive Option

NAI contains two parameters, username and realm written as username@realm. In HA 5.0, both username and realm are case sensitive. When an RRQ with NAI is received from the FA, the HA has to find a match with the configured commands. HA 5.0 tries to find a case sensitive match for both username and realm.

The Realm Case Insensitive feature enables you to match the configured commands against RRQ NAIs with case insensitive realm parameters. However, the username is still considered to be case sensitive.

Example 1:

Local Configuration

```
router(config)#ip mobile host nai @sprintpcs.com interface Null0
```

The following NAIs (with different cases of the same realm) are a match is the above configuration.

- mobile1@sprintpcs.com
- mobile2@sprintPCS.com
- mobile3@sprintPCS.COM
- mobile4@SPRINTPCS.COM
- mobile5@sPrInTpCs.cOm

Example 2:

Local configuration

```
router(config)#ip mobile host nai mobile6@sprintpcs.com interface Null0
```

The following NAIs (with different cases of same username) are not a match with the above configuration CLI:

- Mobile6@sprintpcs.com
- MoBiLe6@SPRINTPCS.COM
- MOBILE6@sprintpcs.com

Configuring the Realm Case Insensitive Feature

To enable the Realm Case Insensitive feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile options`	Provides a sub configuration mode for entering MobileIP options.
	`Router(config)# realm case-insensitive`	Enables the Realm Case-Insensitive feature.

Here is an example:

```
HA(config)#ip mobile options
HA(config-ipmobile-options)#realm case-insensitive
```

Here is an example of how to verify the command:

```
router#show ip mobile options
IP Mobility Options information:

Realm (Domain) match is case insenstive
```

Limitations and Restrictions

Following are the limitations and restrictions for this feature:

- RRQs having NAI with realm case insensitive are considered to be from the same MN. For example, “user1@cisco.com” and “user1@CISCO.COM” are considered to be from the same MN.
- Realm Case Insensitive enable/disable cannot be modified when active sessions are present.
- Realm case insensitive does not work for conditional debugging with username **debug condition username** *nai*. To enable conditional debugging for a user, you must use a case sensitive NAI.

FA-HA Auth Extension Mandatory

The HA must be able to force the HA to require the FA-HA Authentication Extension in the MIP RRQ, or otherwise reject the RRQ. This feature rejects any RRQ that does not have an appropriate **ip mobile secure foreign-agent** command configured. Currently if you send an RRQ to the HA and omit the FA-HA Auth Extension, and do not configure the **ip mobile secure foreign-agent** command for this FA IP Address, the RRQ is accepted. This is considered to be a security risk.

Currently, the HA allows the FHAE extension received in an RRQ or revocation messages from Wimax FAs based on local configuration of the **FA Access-Type** command. The HA supports the following command that allows the FHAE in a received MIP RRQ for Wimax FAs:

ip mobile home-agent foreign-agent *fa-address mask* **access-type wimax {enable-fhae | disable-fhae}**

The above command is modified for 3gpp2 access-type by having the keywords **enable-fhae** and **disable-fhae** added for 3gpp2 FAs. To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent foreign-agent {default | {`*`fa-address mask`*`}} access-type {wimax | 3gpp2} [enable-fhae | disable-fhae]`	Configures the FHEA extension received in an RRQ or revocation messages from a Wimax or 3gpp2 FA.

Here are some configuration details:

- Whenever the command options are modified for the same address and mask values of FAs from option-less/enable-fhae to disable-fhae, then the HA will clear already stored FA-HA keys for those FAs.
- When the Access-type option is modified for the configured address and mask values, then the HA deletes the already stored FA-HA keys.

RRQ Processing on HA

The following scenarios are indicate how the HA processes the RRQ in these scenarios

SCENARIO -1

FA access-type is not configured with **enable-fhae** or **disable-fhae** indicated in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

Configure FA-HA key values for 3gpp2 FAs locally on the HA using the following commands:

ip mobile secure foreign-agent *start-ip end-ip* spi …..

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is configured locally
RRP is sent successfully with FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ does not have FHAE.

a. FA-HA key is configured locally
RRP is sent with error code 132 with FHAE.

b. FA-HA key is not configured locally
RRP is sent successfully without FHAE.

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is already derived from HA-RK (or) HA-RK is already present.
Access-Request is not sent for HA-RK, but may be sent for other purpose.
RRP is sent successfully with FHAE.

b. FA-HA key is not present and HA-RK is not present. Access-Request is sent.
- HA-RK is downloaded.
- RRP is sent successfully with FHAE.

c. HA-RK is not downloaded.

- RRQ is dropped and RRP is not sent.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is already derived from HA-RK. or earlier RRQ from this FA has FHAE.
RRP is sent with error code 132 with FHAE.

b. FA-HA key is not present. None of the RRQs from this FA have FHAE.
RRP is sent successfully without FHAE.

SCENARIO -2

FA access-type is configured with **enable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

To configure the FA-HA keys for 3gpp2 FAs locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent` *start-ip end-ip* spi	Configures the FA-HA keys for 3gpp2 locally on the HA.

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is configured locally
RRP is sent successfully with FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ does not have FHAE.

a. FA-HA key is configured locally
RRP is sent with error code 132 by appending FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code - 132 without FHAE.

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is already derived from HA-RK (or) HA-RK is already present.
Access-Request is not sent for HA-RK, but may be sent for other purpose.
RRP is sent with FHAE.

b. FA-HA key is not present and HA-RK is not present.
Access-Request is sent.

a. HA-RK is downloaded.
RRP is sent with FHAE.

b. HA-RK is not downloaded.
RRQ is dropped and RRP is not sent.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is already derived from HA-RK. The earlier RRQ from this FA has FHAE. (This result is the same even if the FA-HA key is deleted because of the HA-RK lifetime expiry. Using FHAE once for this FA is enough for this condition).
RRP is sent without FHAE - (FA Failed Authentication error code).

b. FA-HA key is not present.
Irrespective of whether HA-RK is downloaded or not. RRP is sent with error code 132 without FHAE.

SCENARIO -3

The FA access-type is configured with **disable-fhae** using the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

To configure the FA-HA key values locally on HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys locally on the HA.

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is not configured locally
Access-Request is not sent (for obtaining FA-HA key).
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ doesn't have FHAE.

a. FA-HA key is not configured locally
RRP is sent successfully (without FHAE).

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is not present and HA-RK is not present.
Access-Request is sent.
a.HA-RK is downloaded.
b.RRP is sent without FHAE.

b. HA-RK is not downloaded.
RRP is sent without FHAE.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is not present.
RRP is sent without FHAE.

Processing and Initiating Revocation Messages

SCENARIO -1

The FA access-type is not configured with **enable-fhae** or **disable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

To configure the FA-HA key values for 3gpp2 FAs locally on HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys for 3gpp2 locally on the HA.

- For 3ggp2 FAs, the HA sends a Registration Revocation Message to the FA by authenticating the message with/without FHAE-based FA-HA key configuration
- For Wimax FAs, the HA does not send a Registration Revocation Message to the FA if the HA-RK key timer expires, or if the HA-RK key or FA-HA key are unavailable.
- The HA drops the received Registration Revocation Message from the FA if the Registration Revocation Message has FHAE and the HA does not have a FA-HA key locally for the corresponding FA. This is true for both 3gpp2 and Wimax FAs.
- The HA drops the received Registration Revocation Message from the FA if the received message does not have FHAE, but is configured with the FA-HA key locally on the HA for 3gpp2, or if the key is already derived for Wimax.
- For other cases, the HA processes or initiates the Registration Revocation Messages.

SCENARIO -2

The FA access-type has an option with **enable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

To configure the FA-HA keys for 3gpp2 FAs locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys for 3gpp2 locally on the HA.

- For 3ggp2 FAs, the HA does not send a Registration Revocation Message to the FA if the FA-HA key is not available locally.
- For Wimax FAs, the HA does not send a Registration Revocation Message to the FA if the HA-RK key timer expires, or if the HA-RK key or FA-HA key is unavailable.
- The HA drops the received Registration Revocation Message from the FA if the received message does not have FHAE, but is configured with FA-HA key locally on the HA for 3gpp2, or the key is already derived for Wimax.
- For other cases, the HA initiates the Registration Revocation Messages +vely.

SCENARIO -3

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

To configure FA-HA key values locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA key values locally on the HA.

- The HA drops the received Registration Revocation Message from the FA if the Registration Revocation Message has FHAE. This is true for both 3gpp2 and Wimax FAs.
- For other cases, the HA initiates the Registration Revocation Messages +vely.

Absolute Timeout Per NAI

In case of data-path idle timer, the user gets deleted whenever it remains idle (no traffic) for the configured interval. But, when started, the absolute timer removes the user, even though the user is active.

This feature sets the absolute timeout for a session either locally, or through a Radius Access Accept, to disconnect the user's session when the timer expires regardless if the user sends traffic, or not. Currently, the HA supports the AAA attribute session-timeout [27] in case of hotline users. The same attribute is extended for the absolute-timer.

The absolute-timer should be initiated during Registration only and should never get modified until the binding is deleted. If the absolute-timer is not received during registration, but it is received during re-registration, then the absolute timer is not started. The absolute-timer has meaning only for initial registration.

The absolute-timer runs independent of the hotline timer. Once configured, the absolute timer clock continues and will delete the binding when it expires.

Redundancy is supported, and the absolute timeout value needs to be synched to the standby.

Configuring the Absolute Timeout Feature

To enable the HA to set the absolute timeout for a session, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *realm* `absolute-time` *interval-in seconds*	Configures the **absolute-time** locally on HA. When Session- Timeout [27] gets downloaded from the AAA, it takes a higher precedence and will overwrite the locally configured **absolute-time** value.

Verifying the Configuration

Here are some examples to help you verify and troubleshoot the configuration:

For 3GPP2 binding, the output will be as follows:

```
# show ip mobile binding

Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:52
    Flags sBdmg-T-, Identification CD735149.00000005
    Tunnel0 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Tunnel0 Output ACL: p1_test - ACL is empty or not configured
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
```

```
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:52
    Traffic Plane Id:6
```

For WiMAX binding, the output will be as follows:

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
sony6@cisco.com (Bindings 1):
    Home Addr 65.0.0.3
    Care-of Addr 50.1.1.90, Src Addr 50.1.1.90
    Lifetime granted 02:00:00 (7200), remaining 01:59:07
    Flags sBdmg-T-, Identification CD7352EA.00000006
    Tunnel0 src 14.0.0.2 dest 50.1.1.90 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: WiMAX(802.16e)
    Acct-Session-Id: 0x00000004
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:02:00 (120), remaining 00:01:07
    Traffic Plane Id:5
```

Incase of both hotline timer and absolute timer are present for the binding, the output will be:

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:49
    Flags sBdmg-T-, Identification CD7358E6.00000005
    Tunnel1 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000009
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Hotline session granted 00:01:00 (60), remaining 00:00:49
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:49
    Traffic Plane Id:6
```

The following new debug statements will appear when this feature is configured.

```
MobileIP: Absolute timer expired for MN derath5@cisco.com
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000009
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel1 src 14.0.0.2 dest 50.1.1.92
MobileIP: Delete database info. for MN 65.0.0.2
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel0 src 14.0.0.2 dest 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000007
```

```
MobileIP: Delete database info. for MN 65.0.0.2
```

Restrictions and Limitations

- The HA should not delete the binding on the standby CP. Otherwise, the binding deletion from the active will fail and appear in the error statistics.

  The following special case/race conditions are handled separately (for example, one race condition):

  - A binding is created on the active/standby.
  - The timer expires on the active and standby.
  - The binding is deleted from active, but not from the standby because the timer expired.
  - A switchover occurs before the binding deletion event is sent from the active to the standby.
  - The standby becomes the active and has a binding for which the absolute timer expired.

  To handle the above case, the absolute-timer is stopped and re-started on the standby for the interval with which it initially started. After this interval expires, the binding is deleted.

Support for ACLs on Tunnel Interface

The Cisco Tunnel Templates feature allows the configuration of ACLs on statically created tunnels to be applied to dynamic tunnels brought up on the Home Agent. A tunnel template is defined and applied to the tunnels between the Home Agent and PDSN/Foreign Agent.

Configuring Mobile IP Tunnel Template Feature

To enable the Mobile IP Tunnel Template feature, perform these tasks:

	Command	Purpose
Step 1	`Router(config)# interface tunnel` *10* `ip access-group 150`	Configures an interface type and enters interface configuration mode. **tunnel** interface; a virtual interface. The number is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
Step 2	`Router(config)# access-list 150 deny any  10.10.0.0 0.255.255.255` `access-list permit any any`	Configures the access list mechanism for filtering frames by protocol type or vendor code
Step 3	`Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1`	Configures the Home Agent to use the template tunnel.

Here is a sample configuration used to block certain traffic using the template tunnel feature:

```
interface tunnel 10
ip access-group 150 in -------> apply access-list 150
access-list 150 deny any  10.10.0.0 0.255.255.255
access-list permit any any------> permit all but traffic to 10.10.0.0 network
ip mobile home-agent template tunnel 10 address 10.0.0.1
```

Note If you enable the Mobile IP Tunnel Template feature and remove the tunnel interface from the configuration, you should also manually remove the corresponding **mobileip tunnel template** command. If necessary, you can reconfigure the **mobileip tunnel template** command after you configure a new tunnel interface.

Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY

The Cisco Home Agent supports the following 3GPP2 standard attributes:

MN-HA-SPI (26/57)

MN-HA-SHARED-KEY (26/58)

The following procedure illustrates this support:

Step 1 The HA receives an RRQ from the PDSN/FA

Step 2 The HA sends an Access Request to AAA. The HA adds the MHAE SPI of the RRQ to the Access Request as MN-HA-SPI(26/57) attribute.

Step 3 The AAA server matches the MN-HA-SPI (26/57) against the corresponding MN-HA-SHARED-KEY (26/58).

Step 4 The AAA server includes that MN-HA-SHARED-KEY (26/58) in the access reply.

Step 5 The HA authenticates the MHAE of RRQ using the downloaded shared key MN-HA-SHARED-KEY (26/58).

Note If the MN-HA key and SPI are downloaded from AAA using 3gpp2 attributes [57/58], then the HA authenticates MHAE using MD5 algorithm only.

User Profiles

The Home Agent maintains a per NAI profile that contains the following parameters:

- User Identification - NAI
- User Identification - IP Address
- Security Associations
- Reverse Tunnel indication - the parameter specifies the style of reverse tunneling that is required for the user data transfer with Mobile IP services.
- Timestamp window for replay protection
- State information is maintained for all Registration Request flags requested, and then granted (for example, S|B|D|M|G|V flags).

The profile, identified by the NAI, can be configured locally or retrieved from a AAA server.

Additionally, the Home Agent supports an intelligent security association caching mechanism that optimizes the session establishment rate and minimizes the time for session establishment.

The Home Agent supports the local configuration of a maximum of 200000 user profiles; on the SAMI, the HA supports 6 x 200000 user profiles. The User profile, identified by the NAI, can be configured locally, or retrieved from a AAA server.

Mobility Binding Association

The mobility binding is identified in the Home Agent in the following ways:

- For static IP address assignment, NAI+IP
- For dynamic IP address assignment, NAI
- The **show ip mobile binding** command will show mobility binding information for each user.

The binding association contains the following information:

- Care-of-Address
- Home address
- Lifetime of the association
- Signaling identification field

MS Traffic Redirection in Upstream Path

This feature allows any traffic received from a mobile node to be redirected to the next-hop address in the upstream path. Even mobile node to mobile node traffic is sent outside of the Home Agent, and gets routed back from the external device. The feature can be configured on a per realm basis, which allows that each realm can have a different next hop IP address. This means that only NAI-based hosts are supported; IP address-based hosts are not supported in the redirection. Redundancy is also supported for this feature.

HA Binding Update

When a mobile first registers for packet data services, a PPP session and associated Mobile IP flow(s) are established at the PDSN. In the event of an inter-PDSN handoff, another PPP session is established at the target PDSN, and the mobile registers with the Home Agent using the new PDSN/FA. If PPP idle-timeout is configured on the PDSN virtual-template, the maximum mobile IP lifetime advertised to the mobile will be 1 second less than the idle-timeout.

Idle, or unused PPP sessions at a PDSN/Foreign Agent consume valuable resources. The Cisco PDSN/Foreign Agent and Home Agent support Binding Update and Binding Acknowledge messages to release such idle PPP sessions as soon as possible. In the event of an inter-PDSN handoff and Mobile IP registration, the Home Agent updates mobility binding information for the mobile with the Care-of-Address (CoA) of the new PDSN/FA.

If simultaneous bindings are not enabled, the Home Agent sends a notification in the form of a Binding Update message to the previous PDSN/FA. The previous PDSN/FA acknowledges with a Binding Acknowledge, if required, and deletes the visitor list entry for the Mobile IP session. The previous PDSN/FA initiates the release of the PPP session when there are no active flows for that mobile station.

Note You can configure the Home Agent to send the binding update message on a global basis.

Note This feature works with a Cisco FA that has bind update enabled on the box. Security association between the FA and HA has to be configured on both the boxes for this feature to be enabled.

Selective Mobile Blocking

You might want to block access to a specific mobile for reasons such as prepaid quota is over, service is disabled due to non-payment of bills, or other reasons. You can accomplish this by adding the "mobileip:prohibited" cisco-avpair attribute to the user profile on AAA server. When the "mobileip:prohibited" attribute is returned to Home Agent in access accept, the behavior is as follows:

- If the AAA server returns "mobileip:prohibited=1" in an access accept, and if the MN-HA Security Association for the mobile is configured on the AAA server and also returned to Home Agent in an access accept, the Home Agent sends a registration request (failure) with error code 129 (Administratively Prohibited) to the MN.
- If the AAA server returns "mobileip:prohibited=0" in an access accept, or if the attribute is not returned to the HA in an access accept, the HA performs normal processing of the registration request.

Note The "mobileip:prohibited" attribute should not be set to any value other than 0 and 1.

Support for Mobile Equipment Identifier (MEID)

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. It is a globally unique 56-bit identification number for a physical piece of mobile station equipment. In the interim period though, both the attributes need to be supported on the Home Agent.

The MEID NVSE will be appended by the PDSN node to the Mobile IP RRQ. When the MEID NVSE is received on the HA, and the **ip mobile cdma ha-chap send attribute A3** command is configured, the MEID value is included in the HA-CHAP access request.

Setting Fragmentation Size of First Packet With Offset=0

This feature allows you to set the first fragment size to avoid further fragmentation of the second fragment in the network. Also, when IP fragmentation happens, the first fragment may not include the L4 header information of the inner packet. This could cause the firewalls on the network that does the deep inspection up to L4, to drop the first fragment.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router#`**`ip fragment first minimum size`** *`size`*	Sets the first fragment size to avoid addtional fragmentation. The range is *8-560* bytes. The size includes only the payload, and does not include any header.

Note The "payload size" must be in multiples of 8 bytes. Otherwise, the command is rejected with the following error: "%% First fragment payload size is not in multiples of 8 bytes"

This is an IP level command, and size configuration considers only the payload of the IP packet.

For example, if you configure the first fragment size as 48 bytes, it creates the first fragment with the size of 68 bytes including the 20 byte IP header.

In case of an IP-IP tunnel packet, the configured payload size includes inner the IP header. For fragmentation code, the inner IP is seen as the payload to the outer IP header.

- The command configuration only indicates the minimum value for the payload of the first fragment. If the existing fragmentation mechanism in CEF selects the first fragment larger than the configured value, then the configuration is not enforced. Otherwise, the BWG will generate more fragments than expected.
- Also, if the configured first fragment size is more than the MTU of the output interface, the configured value is not enforced.

The following examples illustrate how the packet would be for IP and IP-IP tunnel packet:

```
router(config)# ip fragment first minimum size 80
IP Packet:

10:27:59.660 IST Mon Apr 13 2009                Relative Time: 2.990258
Packet 8 of 26                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x0092,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x582D (OK)
      Source: 50.1.1.200,     Dest: 13.2.2.15

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x1A45 ERROR: C661
      Identifier: 006A,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E794 B5A4 ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   20 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   40 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   60 : ABCD ABCD ABCD ABCD ABCD ABCD ............


IP-IP tunnel packet:
20:39:40.394 IST Sun Apr 12 2009                Relative Time: 2.967188
Packet 7 of 22                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x8008,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 4 (IP-IP),   Checksum: 0xD9F5 (OK)
      Source: 14.0.0.1,     Dest: 50.1.1.150

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 1500,   ID: 0x0086,   Flags-Offset: 0x0000
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x40D0 (OK)
```

```
      Source: 50.1.1.200,     Dest: 65.0.0.2

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x72CB ERROR: 7C6A
      Identifier: 005E,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E49E 6020 ABCD ABCD ABCD ABCD ABCD ABCD
```

Conserve Unique IP ID for FA-HA IP-in-IP Tunnel

This feature supports several hundred thousand sessions in the Single IP architecture. This is achieved by setting the unique ID in the IP header only when the packet is likely to fragment. Otherwise, the ID field in the IP header should be set to **0**.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router#`**`ip mobile tunnel ip-ip conserve-ip-id threshold`** *`value`*	Sets a unique IDin the IP header when the packet is likely to fragment. The threshold-value range is *576-1500*, and indicates the outer IP packet size. This feature is only supported for the IP-IP tunnel.

When you configure the **ip mobile tunnel ip-ip conserve ip-id threshold** command, if the packet size is more than the **threshold** *value*, it is sent with a unique IP ID in the outer IP header. Otherwise, the identification field is set to **0**. If you set the threshold to 1400 bytes, then packets with size 1401 and above are sent out with a unique IP ID.

This functionality is not the default behavior, and needs to be enabled through this command. Additionally, there is no default threshold value.

VSE Support for China Telecom Attributes

In HA Release 5.1 (which is a single IP architecture), the following changes are made as part of this feature support:

- Ensure that syncing of these NVSEs / attributes between the active and standby is working properly with the SR infrastructure introduced in HA 5.0.
- Ensure that syncing these NVSEs between CP and TP is correct.
- Ensure that the interface with accounting is working properly.
- Ensure that the **show ip mobile binding** output displays the attributes indicating this information.

  Here is sample output:

```
Active-HA#sh ip mobile binding
    Mobility Binding List:
Total 1
ct-cisco@cisco.com (Bindings 1):
        Home Addr 60.0.2.1
    Care-of Addr 4.0.2.3, Src Addr 4.0.2.3
    Lifetime granted 00:33:20 (2000), remaining 00:33:15
    Flags sbdmg-t-, Identification C1F3C1D5.0000000F
    Tunnel1 src 40.0.11.20 dest 4.0.2.3 reverse-allowed
    Routing Options -
```

```
Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
Acct-Session-Id: 0x00000005
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
Correlation Id cisco-ha(vendor id 20942)
Calling Station Id cisco
Served MDN CT-MDN
Charging Type 0x00000001
Traffic Plane Id:7
```

The following attributes are supported as part of this feature.

- Correlation-Id
- Calling-Station-Id
- Served-MDN
- Charging-Type
- HA-Service-Address

Also, as part of this feature support, interactions with the FA and AAA server are slightly modified. The following sub-sections provide additional details.

Interactions with FA

With this feature support, the HA processes the following attributes that are received in RRQ:

- **Calling-Station-Id**

  The HA supports processing of the CT NVSE Calling Station ID attribute received in an RRQ. This enables the PDSN/FA to send the user's IMSI to the HA as a CT NVSE attribute.

- **Correlation-Id**

  The HA processes the received Correlation-Id from the FA in the format of defined in RFC 3115 for Vendor specific attributes for MobileIP.

  When the HA receives new values for the correlation-id or calling-station-id attributes in an RRQ during re-registration, the HA sends an Accounting Stop and Start for the MIP session.

Interaction with AAA

The HA will deal with the following attributes during the interaction with AAA for authentication and Accounting,

- **Correlation-Id**

  The received Correlation-Id in RRQ is sent in Accounting Start/Stop/Interim Messages to the AAA server. This attribute is not included during Authentication with AAA.

- **Calling-Station-Id**

  The received Calling-Station-Id in RRQ is sent in an Access-Request during Authentication with AAA for MN subscriber. This attribute is also sent in Accounting Start/Stop/Interim Messages to AAA server. The HA sends the Calling-Station-Id to AAA in the format of standard RADIUS Attribute [31] , as defined in RFC 2865.

- **Served-MDN**

  The HA receives the Served MDN value in an Access-Accept after successful authentication with the AAA server. The received attribute is sent in Accounting Start/Stop Messages only to the AAA for accounting purposes.

- **Charging-Type**

  The HA receives the Charging-Type value in an Access-Accept after successful authentication with the AAA server. The received attribute is sent in Accounting Start/Stop messages only to the AAA for accounting purposes.

  Charging-Type values include the following:

  - 0x00000001- Post-paid accounting
  - 0x00000002- Pre-paid accounting
  - 0x00000003- both post-paid and pre-paid accounting

- **HA-Service-Address**

  The HA sends the user's HA service address to the AAA in an accounting-start message.

Table 16-1 illustrates how the HA incorporates the attribute values in various Radius messages (RFC 2865 and 2866) during interaction with AAA.

Table 16-1 HA Attributes in Radius Messages During AAA

Attribute	Attribute Value	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Calling-Station-Id	31	0-1	0	0-1	0-1	0-1
Correlation-Id	26/5535/44	0	0	0-1	0-1	0-1
Served-MDN	26/ 20942/ 100	0	0-1	0-1	0-1	0
Charging-Type	26/ 20942/ 101	0	0-1	0-1	0-1	0
HA-Service-Addres	26/5535/7	0	0	0-1	0-1	0

Support for Alternative MN Identifier

Currently, the Home Agent uses NAI to uniquely identify the subscriber. In the China Telecom operator network, all mobile nodes have the same NAI and they are distinguished by Calling Station Identifier (CLID). So, the Home Agent is enhanced to use other attributes to uniquely identify the subscriber. For China Telecom, the alternative MN identifier is the CLID.

The CLID format specification is a subset of the NAI format. In CLID mode, the HA uses CLID for binding identification within the system. Thus, two RRQs that carry the same value in NAI but different values in CLID are identified as two different bindings.

For Authentication, Authorization and Accounting purposes, the realm portion of NAI received in the RRQ is used to identify configurations in the system.

In this mode, if the HA receives a RRQ without the CT CLID NVSE, the HA rejects the RRQ, and the appropriate counter (Bad Request) will be incremented.

The HA supports either NAI, or CLID-based binding identification (based on global configuration). Dynamic change of alternative MN identifier option with active bindings on the system is not allowed.

To configure this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent options`	(Optional) Enables the configuration of IP Mobile Home Agent options, and enters IP Mobile Home Agent option configuration submode.
Step 2	`Router(config-ipmobile-ha-options)#mn-identifier calling-station-id`	(Optional) Enables the CLID as an Alternative Mobile Node identifier. You cannot enable / disable this CLI if there are active bindings in the system.

To verify the configuration, perform the following tasks:

	Command	Purpose
Step 1	`Router# show ip mobile binding`	Displays the mobility binding table.

Here is an example:

```
router#sh ip mob bind
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
111111111111450 (Bindings 1):
    Home Addr 1.1.1.14
    Care-of Addr 10.5.1.2, Src Addr 10.5.1.2
    Lifetime granted 00:08:20 (500), remaining 00:05:17
    Flags sbdmg-t-, Identification CDE8617E.00000008
    Tunnel0 src 86.6.6.6 dest 10.5.1.2 reverse-allowed
    Routing Options -
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit set
    Acct-Session-Id: 0x00000015
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Correlation Id 8(vendor id 20942)
    Calling Station Id 111111111111450
    NAI  ctc_user8@ispxyz.com <--- RRQ nai for this binding.
    Traffic Plane Id:4
```

Support for Call Admission Control (CAC)

Currently, the number of bindings and amount of memory usage are considered for calculating load balancing in HA-SLB. The existing dynamic feedback protocol (DFP) weight calculation equation can be modified by considering the frequency of calls per second (CPS) and throughput parameters on each real server (HA).

The CPS on the HA can be calculated every minute, and is called Usage CPS. Additionally, it can be configured to some maximum value (Available CPS) that can be handled by HA. If the Usage CPS equals the Available CPS, then the HA real server will return less weight to SLB.

As it is difficult to calculate throughput on router and it can be solved by usage of interrupt CPU for packet handling.

From the above two parameters, the equation looks like this:

```
dfp_weight = (Maxbindings - NumberofBindings)*(cpu+mem)*
(Available cps - Usage cps) *dftp_max_weight / (Maxbindings*32*Available cps)
```

Configuring CAC on the HA

To configure the maximum number of bindings that are allowed on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent max-binding` *max-binding-value*	Limits the number of bindings that can be opened on the HA. The default value of max-binding-value is 235,000.

Congestion Control Feature

In Cisco Mobile Wireless Home Agent Release 5.0, the congestion control feature requires that the call admission control algorithm implemented by the Home Agent is modified to take action when it is determined that the congestion state is reached.

You can configure the DFP weight to determine when congestion occurs. Typically, the DFP value corresponds to 70% congestion state. The DFP weight, by default, is in the range **0-24**. You can configure the max weight to have a required range of the values. **0** corresponds to maximum resources used, and the max scale value indicates that resources are 100% available.

The DFP value used is calculated solely for the control processor in the Single IP model. It is not expected that Traffic Plane processor resource usage will contribute to congestion.

When the congestion state is reached, four possible actions can occur:

- Reject: Reject any new call attempts. The rejection is indicated by sending a MIP Registration Reply with error code 130 (insufficient resources).
- Abort: Reject any new call attempts and abort any “in progress” calls. In-progress means any MIP registration where the Registration Request has been received and the Registration Reply has not yet been sent. The rejection is indicated by sending a MIP Registration Reply with error code 130 (insufficient resources).
- Redirect: Reject any new call attempts and abort any “in progress” calls. In-progress means any MIP registration where the Registration Request has been received and the Registration Reply has not yet been sent. The rejection is indicated by sending a MIP Registration Reply with error code 136 (unknown Home Agent address). The Home Agent address field will contain the address of the Home Agent that the call attempt should be redirected to. The to-be-redirected-to-address is configured globally on the Home Agent.
- Drop: Drop existing calls based on Data Path Idle Timer evaluation. Any bindings with the data path idle time that surpassed a configured value are released. This event sends a Resource Revocation message, if configured. If Resource Revocation is not configured, the binding is silently removed as if a local binding clear was requested.

Note Only one action is configurable at one time. If you try to configure a second action, that will overwrite the first one.

Configuring the Congestion Control Feature

Perform the following tasks to define the call admission control actions when the congestion trigger occurs:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent congestion` *dfp_weight* **action | reject | abort | redirect** *HA-address* **| drop data-path-idle** *minutes*	Defines the call admission control actions when the congestion trigger occurs.
Step 2	`Router# show ip mobile home-agent congestion`	Displays the following information: • Congestion state—congested or not congested. • Configured value of congestion-threshold = dfp_weight from configured CLI. • Current dfp-value. The current-dfp-value is the average DFP value over the last five minutes.

Additionally, the CISCO-SLB-CLIENT-MIB contains the following information:

- DFP congestion onset threshold above which a Congestion On Trap is generated.
- DFP congestion abatement threshold, which when crossed following congestion generates a Congestion Off trap.
- Current DFP value

Here is sample output for the Congestion Control feature:

```
router#show ip mobile home-agent congestion
Home Agent congestion information :
Current congestion level:  Congested
Configured Action : Reject
Configured threshold : 10
Current DFP value = 7
```

Framed-Pool Standard

Framed-Pool is an AAA attribute that contains the name of the assigned address pool used to assign an address for the user on the HA. In HA3.1, this functionality is supported by a Cisco VSA.

The HAAA sends these attributes in an Access-Accept message to the HA for dynamic/static address allocation. If the HA receives both attributes in an Access-Accept, it can accept one among them as pre-configured on HA.

Perform the following task to configure the framed-pool standard feature:

Step 1	`router# ip mobile home-agent aaa attribute framed-Pool`	Enables the HA to use the Framed-Pool attribute, and contains the Local Pool name returned as part Access-Accept from the RADIUS server.

Here is an example:

```
ip mobile home-agent aaa attribute Framed-Pool
ip local pool haPool 70.1.1.1 70.1.1.254
ip mobile home-agent
ip mobile virtual-network 70.1.1.0 255.255.255.0
ip mobile host nai @cisco.com interface FastEthernet1/0 aaa load-sa
```

Priority-Metric for Local Pool

In order to assign IP addresses to mobile clients, the HA uses local pools configured with a range of IP addresses. Whenever a registration request arrives, the HA authenticates the MN and gets the pool name to assign an IP address. The HA gets the pool name either from its own configuration, or from the Radius Server thru a Cisco-VSA or Framed-Pool attributes.

While configuring for IP local pool, you can have multiple groups, each group can have multiple pools, and each pool can have a multiple range of IP addresses. In a single group you cannot have an overlapping range of IP Addresses. All the addresses under a group are unique.

By default, the request for an IP address contains the pool name (mandatory), static IP address (optional), and an associated username (optional). Initially all the IP addresses are put in a free pool and from there each IP address is assigned. Whenever you are assigning IP address, you should associate an IP address with the given username.

You can also add priority to the addresses to select a desired range of IP addresses from the pool for the new requests. Once all of the subscribers move to the new addressing scheme, the old addressing (low priority range) can be removed from the system.

Generally, if an IP address is reserved, it will be associated with that user (by userid). If the user disconnects and connects again, the same IP address will be given to that user if it is not used by anyone. This user IP address association is controller by cache-limit along with the pool configuration. So if you change the priority of the addressing scheme, or if a high priority addressing scheme is available with a free address, then the HA assigns a new IP address from the new addressing scheme rather than giving the old reserved IP address. If there is no change in the priority, HA will try to assign the previous IP address.

You can also set and get the priority value through the SNMP MIBS by accessing the same from Network Manager. The new MIB object for priority is added to the “cIpLocalPoolConfigEntry” table to access the priority value. With the new MIB object, you can change the priority of an existing local pool.

Configuring Priority Metric for Local Pool

To configure the Priority Metric for local pool feature perform the following tasks:

Step 1	`router# Router(config)#`**`ip local pool {default |`** *`poolname`*`}` **`[`***`low-ip-address`*` `**`[`***`high-ip-address`*`]] [group`** *`group-name`*`]` **`[cache-size`** *`size`*`] [priority`** *`1-255`*`]` **`[theshold`** *`low-threshold high-threshold`*`]`	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, to generate traps when pool utilization reaches a high or low threshold in percentage. The new option **priority** *1-255* is allows you to assign a priority to a newly created pool, and this priority is used to assign IP addresses.
Step 2	`Router(config)#`**`no ip local pool`** `vsa-pool 1.0.0.201 priority 180`	Unconfigures the pool.

Here is an example:

The HA creates a local pool with default priority as 1 (lowest priority)

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255
```

The HA creates a local pool with priority 100

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255 priority 100
```

Verifying the Configuration

Perform the following task to verify the configuration:

Step 1	`Router#`**`show running-config | include pool`**	Displays the local pool configuration along with its priority only if the priority is not equal to 1 (default and lowest value).

Here is an example:

```
Router# show running-config | include pool
ip local pool frmd-pool 1.0.0.191 priority 20
ip local pool vsa-pool 1.0.0.201 priority 180
ip local pool vsa-pool 1.0.0.211 1.0.0.219
ip local pool vsa-pool 1.0.0.202 1.0.0.209 priority 100


router# show ip local pool

 Pool          Begin         End           Free  In use  Priority
 frmd-pool     1.0.0.191     1.0.0.191        1       0        20
 vsa-pool      1.0.0.201     1.0.0.201        1       0       180
               1.0.0.211     1.0.0.219        9       0         1
               1.0.0.202     1.0.0.209        8       0       100
```

Mobile IPv4 Host Configuration Extensions RFC4332

This section describes the Mobile IP host configuration extensions as implemented in IOS.

An IP device requires basic host configuration to be able to communicate. For example, it typically requires an IP address and the address of a DNS server. This information is configured statically or obtained dynamically using Dynamic Host Configuration Protocol (DHCP), or Point-to-Point Protocol/IP Control Protocol (PPP/IPCP). However, both DHCP and PPP/IPCP provide host configuration based on the access network. In Mobile IPv4, the registration process boots up a Mobile Node at an access network, also known as a foreign network. The information to configure the host needs to be based on the home network. The Mobile Node at a foreign network needs to get the IP address, home subnet prefix, default gateway, home network's DNS servers in the boot up of the network interface.

When the Mobile Node needs to obtain its host configuration, the Host Configuration Request VSE is appended to the Registration Request. This VSE indicates to the Home Agent that either all, or selected host configuration VSEs need to be appended to the Registration Reply. If the Home Agent retrieves the information from a DHCP server in Proxy DHCP mode, then the DHCP Client ID and DHCP Server extensions are appended in the Registration Reply. These DHCP-related extensions are populated with values that had been used in the DHCP messages exchanged between the Home Agent and the DHCP server. The VSEs are authenticated as part of the registration message using any of the authentication mechanism defined for Mobile IP.

The following Cisco vendor-specific extensions provide the host configuration for a Mobile node. The "Host Configuration Request" extension is allowed only in the Registration Request.

The rest of the extensions are appended in the Registration Reply.

- Host Configuration Request: request for host configuration information from the Mobile Node to the Home Agent.
- Home Network Prefix Length: the length of the subnet prefix on the home network.

- Default Gateway: the default gateway's IP address on the home network.
- DNS Server: the DNS server's IP address in the home network.
- DNS Suffix: the DNS suffix for hostname resolution in the home network.
- DHCP Client ID: the DHCP Client ID used to obtain the IP address. When the Mobile Node returns home and is responsible for managing its own address, this information maps to the Client identifier option.
- DHCP Server: the DHCP server's IP address in the home network.
- Configuration URL: the URL for the Mobile Node to download configuration parameters from a server.

Note The DNS suffix is not appended in RRP when it is downloaded from the DHCP Server.

WiMAX AAA Attributes

Cisco Home Agent Release 4.0 and above adds support for AAA Authorization and Accounting attributes. The following sections describe the attributes, and provide information on specific attribute support.

HA-AAA Authorization Attributes Support for WiMAX

Following HA-AAA attributes will be added in order to extend support for WiMAX.

- Framed IP Address: When the **ip mobile home-agent send-mn-address** command is configured, the home address received in the MobileIP RRQ is sent as the value of the Framed-IP-Address attribute in Access-Request messages.

Note In the Home Agent Release 4.0 software, the Framed-IP-Address attribute is missing in the access request when opening a MIP flow (Wimax).

- WiMAX Capability: This attribute identifies the WiMax capabilities of the HA, and is sent in all Access-Request messages. It can also be sent by the HAAA in Access-Accept messages. If this attribute is present in an Access-Accept message, it can contain only the Accounting Capabilities sub-TLV, which indicates the accounting capabilities selected by the server for the sessions. It is expected that the accounting capabilities returned by the HAAA in the Access-Accept match the value specified by the HA sent in the Access-Request. Currently, the HA does not process the WiMAX Capability VSA received in an Access-Accept, and performs no verification if the accounting capabilities match.
- HA-IP-MIP4: This attribute identifies the IP address of the HA making the request. This attribut is included in all Access-Request messages from the HA. For existing bindings (Access-Requests corresponding to re-registration and deletion), it's value is set to the home agent address of the binding. For new bindings, the value of this attribute is set to the HA IP address (not Home Address) that is assigned for the binding from the HA configuration that is also sent as the Home Agent IP address in RRP. Refer to the Configuring Home Agent IP Address for the Bindings section.
- RRQ-HA-IP: the HA includes this attribute in an Access-Request message if the IP address in the Home Agent field of the MobileIP RRQ is different from the IP address of the HA. If present, its value is set to the Home Agent IP address in the Mobile IP RRQ.

- MN-HA-MIP4-KEY: This attribute identifies the MN-HA key used for MIP4 procedures. This attribute is included in an Access-accept message, and it is similar to MN-HA-SHARED-KEY. The HA computes the MN-HA Authentication Extension based on the MN-HA MIP4 key for WiMAX subscribers.
- MN-HA-MIP4-SPI: This attribute identifies the MN-HA SPI used for MIP4 procedures. This attribute is included in an Access-Request message, and it is similar to MN-HA-SPI.

Table 16-2 identifies the WiMAX AAA Authorization attributes for the Home Agent.

Table 16-2 WiMAX AAA Authorization Attributes

Attribute Name	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject	Supported in HA 4.0 and above
Message-Authenticator	80	Message Authenticator to integrity protect the AAA message	1	0	1	0	Yes
WiMAX Capability	26/1	Identifies the WiMAX Capabilities supported by the HA. Indicates capabilities selected by the RADIUS server.	1	0	0-1	0	Yes
CUI (Chargeable User Identity)	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1	0	0-1	0	Yes
AAA-Session-ID	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	0-1	0	1	0	Yes
HA-IP-MIP4	26/6	The IP address of the HA making this request	0-1	0	0	0	Yes
RRQ-HA-IP	26/18	The HA-IP address contained in the Registration Request or Binding Update.	0-1	0	0	0	Yes
MN-HA-MIP4-KEY	26/10	The MN-HA key used for MIP4 procedures.	0	0	1	0	Yes
MN-HA-MIP4-SPI	26/11	The SPI associated with the MN-HA-MIP4-KEY.	1	0	1	0	Yes
RRQ-MN-HA-KEY	26/19	The MN-HA-KEY that is bound to the HA-IP address as reported by RRQ-HA-IP attribute.	0	0	0-1		Yes
HA-RK-Key-Requested	26/58	Indicates that the HA-RK-KEY attribute should be included in the Access-Accept.	1	0	0	0	Yes
HA-RK-KEY	26/15	HA-RK key used to generate FA-HA keys.	0	0	0-1	0	Yes
HA-RK-SPI	26/16	The SPI associated with the HA-RK.	0-1	0	0-1	0	Yes
HA-RK-Lifetime	26/17	HA-RK key used to generate FA-HA keys for MIP4 operations.	0	0	0-1	0	Yes
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1	0	Yes

AAA Attributes for "ip mobile host/realm"

The following attributes will be supported as part of this feature.

- Attribute "data-path-idle"—This is to set the data-path idle timer per Mobile basis as a AAA attribute. It would be downloadable as a Cisco AV pair. If the value is downloaded from AAA and also configured locally, then AAA downloaded value takes precedence. In the RSIM subscriber profile, the config would look like this.

  vsa cisco generic 1 string "mobileip:data-path-idle=300"

  Notes:

  - If the binding were already created with AAA attribute "data-path-idle" and if the **ip mobile realm** *realm* **data-path-idle** is configured/modified later, then only the bindings that were created without the AAA attribute will be updated. This is to make sure that AAA precedence is still intact.
  - Re-registrations can update the data-path-idle timer.

- Attribute "Nexthop"—This is to set the nexthop IP per Mobile basis as a AAA attribute. This would be downloadable as a cisco AV pair. If this value is downloaded from AAA and also configured locally, then AAA downloaded value takes precedence. In the RSIM subscriber profile, the config would look like this.

  vsa cisco generic 1 string "mobileip:nexthop=1.1.1.1"

  Notes:

  - If the bindings were already created with nexthop downloaded from AAA, and if the **ip mobile realm** *realm* **any-traffic nexthop** *ip* command is configured, the CLI will not be accepted.
  - When **nexthop ip** is configured through CLI with bindings already created, then only the confirmation of the deletion of bindings, the value can be updated.
  - Re-registrations cannot update the downloaded nexthop attribute.

MN and Foreign Agent Authentication

The HA includes the SPI received in the MHAE as the value of the MN-HA-MIP4-SPI attribute in the Access-Request along with HA-IP-MIP4. The value of the MN-HA-MIP4-KEY attribute downloaded from the AAA corresponding to HA-IP-MIP4 and SPI value in the MN-HA-MIP4-SPI attribute is used to verify the MHAE in the Mobile IP RRQ and to generate MHAE for Mobile IP RRP.

The following information is extracted from the Registration Request:

- MN-HA SPI in the MN-HA Authentication Extension.
- HA IP address in Home Agent field.
- Recipient IP address in the Destination IP address field.
- FA-HA SPI in the FA-HA Authentication Extension if this extension is in the message.

The HA includes the MN-HA-MIP4-SPI and HA-IP-MIP4 attributes (which contain the MN-HA SPI and HA IP address, respectively) in the Access-Request that is sent to the AAA server. The Access-Accept from the AAA server includes the MN-HA-MIP4-KEY attribute which corresponds to the two attributes in the Access-Request. The HA sets up the MN-HA security association with the downloaded key. The security association is used to authenticate the MN-HA Authentication Extension in the Registration Request, and for generating this extension in the Registration Reply.

The Registration Request may contain the Home Agent field with IP address set to all ones or zeros to indicate dynamic HA assignment. In this case, the HA includes an additional RRQ-HA-IP attribute, which is set to the Home Agent field value, in the Access-Request. The MN-HA-MIP4-SPI attribute is the same as described before. However, the HA-IP-MIP4 attribute is set to the Recipient IP address instead. The AAA server includes the additional RRQ-MN-HA-KEY attribute (which corresponds to the RRQ-HA-IP attribute) in the Access-Accept. The HA uses this key to authenticate the MN-HA Authentication in the Registration Request. Upon successful authentication, the HA sets up the MN-HA security association with the MN-HA-MIP4-KEY to send the Registration Reply. Subsequent registration authentication uses this security assocation.

In case of CMIP, if the RRQ contains HA IP as ALL-ZERO-ONE-ADDR, then along with MN-HA-MIP4-SPI and HA-IP-MIP4, RRQ-HA-IP is also sent in Access-Request with the value equal to HA IP of RRQ. HA downloads RRQ-MN-HA-KEY for RRQ-HA-IP and MN-HA-MIP4-KEY for HA-IP-MIP4 corresponding to MN-HA-MIP4-SPI. The HA verifies MHAE of Mobile IP RRQ using RRQ-MN-HA-KEY and generates MHAE for Mobile IP RRP using MN-HA-MIP4-KEY.

If a RRQ received from a FA contains FHAE, then Foreign-agent authentication happens for that FA. Also all sub sequent RRQs received from that FA should contain FHAE. For authenticating FA at HA, HA-RK needs to be present at HA. If HA-RK is not present at HA , HA downloads HA-RK from AAA.

The HAAA creates a random 160 bit HA-RK key for each HA-IP. The HA-RK is not based on the MIP-RK generated as a result of a specific EAP authentication. Thus, it is not bound to a individual user or authentication sessions, but to Authenticator-HAAA pairs.

If the HA needs to download HA-RK from AAA, then the HA includes an HA-RK-Key-Request VSA with the value set to 1 in Access-Request to indicate that it expects to receive the HA-RK-KEY attribute in the Access-Accept. The HA-RK-SPI attribute is also included in the Access-Request, and its value is set to the SPI received in the FHAE. The HAAA will return the HA-RK-KEY, HA-RK-SPI and HA-RK-Lifetime attributes in Access-Accept associated with the HA-IP-MIP4 attribute sent in the Access-Request. If one of these attributes is present, then all must be present. If not then HA discards the Access-Accept. This attribute is not included in any of the Accounting (Start/Stop/Interim) messages.

HA-RK Key(26/15), HA-RK SPI(26/16), HA-RK lifetime(26/17) will be synched to standby or redundant HA

Both the HA and the FA (which is most likely co-located with the Authenticator) compute the FA-HA key from the HA-RK as follows:

FA-HA = H(HA-RK, “FA-HA” | HA-IPv4 | FA-CoAv4 | SPI)

Where

H = HMAC-SHA1, specified in RFC 2104, HMAC: Keyed-Hashing for Message Authentication

HA-IPv4 = HA-IP-MIP4 attribute sent in Access-Request. (i.e. Binding Home Agent IP).

FA-CoAv4 = Address of the FA expressed as a 32-bit value as seen by the HA

If the MobileIP RRQ received from the FA contains the FHAE extension, then the FA-HA key generated using the above algorithm along with the SPI is used to validate this extension.

You can display the downloaded HA-RK key, SPI, and lifetime using the following **show ip mobile secure home-agent ha-rk** *ha-ip* command.

Here is an example:

```
router#show ip mobile secure home-agent
HomeAgent HA-RK List:
15.1.1.80:
    SPI 102, Lifetime 00:10:30 (630), Remaining 00:10:24
    Key 31323334353637383930313233334353637383930
```

You can display the generated FA-HA-Keys using the **show ip mobile secure foreign-agent** *fa-ip* command.

Here is an example:

```
router#show ip mobile secure foreign-agent
Security Associations (algorithm,mode,replay protection,key):
14.1.1.28:
    SPI 102,  HMAC-MD5, Timestamp +/- 7, HA-IP 15.1.1.80
    Key b932c46406dcfe411f8bd147103ac53ca0c7fe65
```

The above downloaded HA-RK and generated FA-HA-keys are deleted if the HA-RK lifetime expires. If a new HA-RK key is downloaded before the lifetime expires, both the keys will continue to co-exist and authentication will be successful using any one of the keys. The same keys can be deleted using the **clear ip mobile secure all** command. This command clears all the keys MN, FA and HA-RK, generated and downloaded from AAA.

For WiMAX, it is not possible to configure locally the SPI and the key for MHAE or FHAE verification.

Configuring Home Agent IP Address for the Bindings

There are vairous ways to configure the Home Agent to assign the Home Agent IP address to the bindings. Perform the following tasks to enable this feature:

Step 1	**ip mobile realm @cisco.com vrf** *vrf-name* **ha-addr** ***vrf-ha-address***	Enables inbound user sessions to be disconnected when specific session attributes are presented for a specific realm
Step 2	**ip mobile home-agent dynamic-address** *dynamic-ha-address*	Sets the Home Agent Address field in a Registration Response packet.
Step 3	**ip mobile virtual-network** *virtual-net-start mask* **address** *virtual-net-ha-address*	Defines a virtual network.
Step 4	**ip mobile home-agent address** *global-ha-address*	Enables the IP address for virtual networks.
Step 5	**HA HSRP redundancy virtual IP address** *hsrp-ha-ip-address*	Specifies the HSRP IP address.

The Home Agent IP address for the bindings is selected using the preceding configuration details. The same Home Agent IP address is sent as HA-IP-MIP4 in an Access-Request and the Home Agent IP in RRP. The following logic does not apply to the RRQs for previously existing bindings. For an existing binding, the current Home Agent IP address for the binding is used.

- RRQ HA IP and RRQ destination IP are same.

  HA-IP-MIP4 = RRP HA IP address =

  - *vrf-ha-address* if configured.
  - RRQ destination IP address.

- RRQ HA IP is not equal to RRQ Destination IP (holds true for dynamic HA, RRQ HA IP = 0.0.0.0 or 255.255.255.255).

  HA-IP-MIP4 = RRP HA IP address =

  - *vrf-ha-address* if configured.
  - RRQ HA IP if **ip mobile home-agent address** *global-ha-address* **unknown-ha accept reply** is configured. (not for dynamic HA).
  - *dynamic-ha-address* if configured
  - RRQ destination IP address.
- RRQ HA IP or RRQ Destination IP is a subnet-directed broadcast address (RRQ HA IP is not equal to 255.255.255.255). HA discovery!

  HA-IP-MIP4 = RRP HA IP address =

  - MN is on physical interface (above IP corresponds to a physical interface)

    hsrp-ha-ip-address if configured.

    physical interface ip address.
  - MN is on virtual network (above IP corresponds to virtual network). This assumes one of *virtual-net-ha-address* or *global-ha-address* is configured.

    virtual-net-ha-address if configured.

    global-ha-address.

HA-AAA Accounting Attributes Support for WiMAX

The functionality for AAA Accounting Attributes is as follows:

- The HA sends an Accounting Start record when the first binding for a mobile is created.
- The HA sends and Accounting Stop record when the last binding for a mobile is deleted.
- The HA sends Accounting Update when Handoff occurs.

Table 16-3 identifies the WiMAX AAA Accounting Attributes for the Cisco HA:

Table 16-3 WiMAX AAA Accounting Attributes

Name	Type	Description	Start	Int	Stop
Acct-Multi-Session-Id	50	This identifier is set to the value of AAA-Session-Id which is generated by AAA after successful authentication and delivered to the NAS in an Access-Accept message. It is unique per CSN and is used to match all accounting records within a session.	1	1	1
Framed-IP-Address	8	The IPv4 address assigned to the MS. This identifies the IP-Session.	0-1	0-1	0-1
CUI (Chargeable User Identity)	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1	0-1	0-1
HA-IP-MIP4	26/6	The IP address of the Home Agent.	1	1	1

Table 16-3 WiMAX AAA Accounting Attributes (continued)

Event-Timestamp	55	The time the event occurred.	1	1	1
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS or HA.	0-1	0-1	0-1

Configuring WiMAX Support

By default the HA assumes that all of the bindings are of 3gpp2 access type. For WiMAX, the **per foreign-agent access type** command must be configured (Refer to the Per Foreign-Agent Access-Type Support section). In addition, perform the following tasks to enable WiMAX AAA support:

Step 1	`Router# radius-server vsa send authentication wimax`	Configures the WiMAX VSAs included in RADIUS messages. When this command is enabled, the following following RADIUS attributes will be included in Access-Request messages generated by the HA. • Acct-Interim-Interval (85) • Message-Authenticator(80) • Chargeable-User-Identity(89) • WiMAX Capability (26/1) • HA-IP-MIP4 (26/6) • RRQ-HA-IP (26/18) • MN-HA-MIP4-SPI (26/11)
Step 2	`Router# radius-server vsa send accounting wimax`	Configures the WiMAX VSAs included in RADIUS messages. When this command is enabled, the following following RADIUS attributes will be included in accounting messages generated by the HA. • Acct-Terminate-Cause (49) • Acct-Multi-Session-Id (50) • Acct-Session-Time (46) • Chargeable-User-Identity(89) • Acct-Input-Gigawords (52) • Acct-Output-Gigawords (53) • HA-IP-MIP4 (26/6) • GMT-Time-Zone-Offset (26/3)
Step 3	`Router# ip mobile home-agent send-mn-address`	Configures the standard IETF attributes included in RADIUS messages. When configured, the home address received in the MobileIP RRQ is sent as the value of the Framed-IP-Address attribute in Access-Request messages.

Step 4	`Router# radius-server attribute 55 access-request include`	Includes the Event-Timestamp (55) attribute in Access-Requests.
Step 5	`Router# radius-server attribute 55 include-in-acct-req`	Includes the Event-Timestamp (55) attribute in accounting messages.

Verifying the Configuration

Perform the following task to verify that WiMAX support is enabled:

Step 6	`Router# show ip mob bind`	Indicates when WiMAX capabilities are negotiated during authentication of a subscriber.

Here is an example:

```
Router# show ip mob bind
Mobility Binding List:
Total 15000
MIP-USER12573@ispxyz.com (Bindings 1):
    Home Addr 193.1.1.28
    Care-of Addr 7.0.0.85, Src Addr 7.0.0.85
    Lifetime granted INFINITE
    Flags sbdmg-T-, Identification C9ED9187.10000
    Tunnel3 src 73.0.0.42 dest 7.0.0.85 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Acct-Session-Id: 1677265
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

Reject Framed-IP if Already in Use

The HA currently allocates another IP Address from a configured pool of IPs if the Framed-IP address from AAA is already associated with an existing binding. This new feature in Release 5.2 enables the HA to reject a new session when AAA returns a Framed-IP address that is already allocated to a binding for a session.

With this feature enabled, if AAA response returns a “Framed IP-Addr” that is assigned to a binding, the RRQ is rejected with a error code set to “Insufficient Resources or Admin Prohibited”.

To configure this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)#ip mobile home-agent options`	Enables the configuration of IP Mobile Home Agent options, and enters IP Mobile Home Agent option configuration submode.
Step 2	`Router(config-ipmobile-ha-options)#rrq reject frame-ip in-use`	If enabled, this subcommand rejects the RRQ if the “Framed IP Address” in an Access-Accept is already assigned to a binding.

Support for Acct-Terminate-Cause

In Home Agent Release 4.0, the Acct-Terminate-Cause RADIUS attribute (as defined in RFC 2866 Radius Accounting) was supported, however a value of 0 was always inserted.

In Home Agent Release 5.0, the list of values that follows are supported.

The Value field is four octets, containing an integer specifying the cause of session termination.The termination causes are as follows:

- User Request (1) : User requested termination of service, for example with LCP Terminate or by logging out. - On normal MIP session termination.
- Lost Service (3) : Service can no longer be provided; for example, user's connection to a host was interrupted. - When Resource Revocation is received.
- Idle Timeout (4) : Idle timer expired. - When MIP session is terminated on Idle Timer expiry
- Session Timeout (5) : Maximum session length timer expired. - When MIP session registration timer expires.
- Admin Reset (6) : Administrator reset the port or session. - When binding is cleared by the operator.
- NAS Error (9) : NAS detected some error (other than on the port) which required ending the session. - When RRQ for reregistration is in error or FA-HA AE cannot be verified.
- NAS Request (10) : NAS ended session for a non-error reason not otherwise listed here. - When binding is removed for reason not defined for other values of Terminate-Cause.
- Port Preempted (13) : NAS ended session in order to allocate the port to a higher priority use. - When a session is terminated due to congestion.
- User Error (17) : Input from user is in error, causing termination of session. - When the MN-HA AE cannot be verified on re-registration and the binding is removed.

Note Basic Accounting feature needs to be enabled on the HA in order for this Acct-Term-Cause attribute to be included in Accounting-Stop messages.

Per Foreign-Agent Access-Type Support

This feature enables the HA to know which access-type is supported by a foreign-agent based on the IP address of the foreign-agent. The access-type of a foreign-agent can be either **3gpp2** or **WiMAX**, but not both. Depending on the access-type specified, all authentication and accounting records sent from the HA to the AAA server for all the mobiles under that foreign-agent contain either 3gpp2 or WiMAX attributes, but not both. On reception of Access-accept, the HA processes the attributes based on the access-type specified. If the access-type is not specified for a specific foreign agent address, then the default access-type **3gpp2** is used for all the mobile nodes under that foreign-agent. The default access-type can be changed from **3gpp2** to **WiMAX**.

Configuring Foreign-Agent Access-Type Support

Perform the following tasks to configure support for the Forign-Agent Access type:

	Command	Purpose
Step 1	`Router# ip mobile home-agent foreign-agent { default |{ip-address mask} } access-type {3gpp2 | wimax}`	Selects either **3gpp2** or **wimax** access-type for a subscriber based on the IP address of the foreign agent through which the request came.

This configuration will not be considered if the respective access-type is not configured under RADIUS (**radius vsa send authentication 3gpp2/wimax** for authentication, and **radius vsa send accounting 3gpp2/wimax** for accounting).

Configuration on AAA Server

This section describes the configuration of AAA authentication and accounting attributes on the AAA server. Please note this is a general configuration.

Table 16-4 AAA Authentication and Accounting Attributes on the AAA Server

Attribute	Description
attribute 4 *vsa string*	A unique identifier in the home realm for this Session as set by the HAAA
attribute 6 *ip address as string*	The IPv4 address of the HA for MIP4. This is IP address of the HA making the request.
attribute 10 *ascii or hex corresponding string*	The MN-HA-KEY sent by the RADIUS Server to the ASN (for PMIP) or HA use for MIP4 (MIP or PMIP). It is used by the ASN during PMIP4 to calculate the MN-HAAE. It is sent to the HA to validate the MN-HA-AE (MIP4) and to compute the MN-HAAE for of the MIP4 Registration Response or the AUTH for MIP6 Binding Answer based on the MIP version(MIP4 or MIP6) and the SPI.
attribute 11 *spi hex value* range of hex value- 100-FFFFFFFF	The SPI associated with the MN-HA-MIP4-KEY

Table 16-4 AAA Authentication and Accounting Attributes on the AAA Server (continued)

attribute 15 *ascii or hex corresponding string*	The HA-RK-KEY determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate FA-HA keys.
attribute16 *spi hex value* range of hex value- 100-FFFFFFFF	The SPI used for the HA-RK.
attribute 17 *vsa value*	The lifetime of the HA-RK and derived keys.
attribute 19 *ascii or hex corresponding string*	The MN_HA key sent by the HAAA to the HA to be used to validate the MN-HA-AE of the Mobile IP Registration Request.

Foreign Agent Classification

The Home Agent supports the inclusion of the Proxy Mobile IPv4 Access Technology Type Extension received in a Mobile IP Registration Request. Tech-type values of **3** indicate 802.16e (WiMax) and **7** indicates that 1xRTT/HRPD are supported. If no extension is received the per-Foreign Agent configuration applies. If there is no Per-FA configuration, the global value applies. This defaults to 3GPP2, and can be configured instead to WiMax.

Other values are not supported and the extension is ignored in this case. A single counter is present that indicates the number of times the extension is received with non-supported values. The extension contents are displayed in a debug command that displays mobile messaging contents.

Receipt of tech-type value **3** indicates that the mobile IP registration is for WiMax access. In this case, the actions taken are identical to those for the case when a Foreign Agent is locally configured to support WiMax access.

Receipt of tech-type value **7** indicates that the mobile IP registration is for 1xRTT/HRPD access. In this case, the actions taken are identical to those for the case when a Foreign Agent is locally configured as supporting 3GPP2 access.

The actions taken based on tech-type value take precedence over any locally-configured per-Foreign Agent Access Type configuration. For example, if the locally configured value indicates 3GPP2 and the tech-type value indicates WiMax, then the actions for WiMax are taken.

Note The Access-type of a binding remains the same even if the Home Agent receives different Access Technology Type in Re-registration

MS Traffic Redirection in Upstream

This feature allow any IP traffic received from a mobile node to be redirected to a next-hop IP address in the upstream path. The next-hop IP address is configured on a per realm basis, and is only supported for NAI-based mobile nodes. The same configuration needs to be present both on the active and standby Home Agents for redundancy support.

Configuring MS Traffic Redirection in Upstream Traffic

In addition to the previous configuration details, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm realm any-traffic next-hop next-hop-ipadress`	Sets the next-hop address for the realm. **any-traffic** indicates that any or all traffic in the upstream from the mobile is redirected. **next-hop** indicates the next-hop feature. *next-hop-ip-address* is the IP address of the next-hop, where the packets needs to be redirected to.

Verifying the Configuration

Perform the following task to verify that MS traffic is redirected:

	Command	Purpose
Step 1	`Router# show ip mobile binding`	Displays that the binding is modified, and displays the next-hop address configured for the mobile.

Here is an example:

```
Router#sh ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
xyz1@xyz.com (Bindings 1):
    Home Addr 11.110.1.1
    Care-of Addr 13.1.1.112, Src Addr 13.1.1.112
    Lifetime granted 00:30:00 (1800), remaining 00:29:52
    Flags sbdmg-T-, Identification CAF62BE1.1
    Tunnel0 src 13.1.254.254 dest 13.1.1.112 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled
    Next-hop set for any-traffic to 14.1.1.201
```

MAC Address as Show/Clear Binding Key

In Cisco Mobile Wireless Home Agent Release 5.0, sessions now contain the MAC address of the terminal. This identifier is learned through Mobile IP signaling. The initial registration request includes the MAC address, and re-registration and de-registration may also include the MAC address. This feature allows a network administrator to search for a session, delete a session, and enable debugging for a host based on the MAC. The debugging and syslog messages are contained the MAC address of the terminal whenever applicable.

The MAC address should also be added to the Cisco-Mobile-IP-MIB.

Note The MAC address is unique for an access network technology, and can be learned from the Proxy Mobile IPv4 Access Network Technology Extension. The default value for access network technology is none.

The following commands are changed to include this new field:

Show Commands :

show ip mobile binding mac address: displays the binding information for a host with the specified MAC address. The output includes the MAC address.

Debug Commands :

debug ip mobile host mac address: displays debugging events for a host with the specified MAC address. The messages include the MAC address when applicable.

Clear Commands :

clear ip mobile binding mac address: deletes the mobility binding entry for the host with the specified MAC address.

Data Path Idle Timer

In Cisco Mobile Wireless Home Agent Release 5.0, when there is no data traffic to and from a terminal for a specified period of time (idle time), the session is terminated. This idle time is configurable either on a per-domain basis, or globally. The per-domain configuration takes higher precedence. Revocation messaging triggered by the binding deletion event may occur.

Re-registrations do not reset the idle timer since RRQs are not received on the data path.

For split Control/Data Plane consideration, only the Traffic Processor is aware of the data traffic for a session. It needs to inform the Control Processor if the idle time has been reached.

The data path idle timer information is synchronized between the Home Agents using the Accounting Interim Sync feature.

Perform the following tasks to enable this feature:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *realm* `data-path-idle` *minutes*	Deletes the mobility binding entry in the domain when there is no traffic for a configured period of time (idle time) for a mobility host with NAI that matches the specified realm. The range is 1 - 65535.
	`Router(config)# ip mobile home-agent data-path-idle` *minutes*	Deletes the mobility binding entry when there is no traffic for a configured period of time (idle time). The range is 1 - 65535.

Here is example show output for the Data Path Idle Timer feature:

```
cisco-1@cisco.com (Bindings 1):
    MAC Addr 0000.0001.0000
    Home Addr 5.1.0.1
    Care-of Addr 2.2.2.200, Src Addr 2.2.2.200
    Lifetime granted 10:00:00 (36000), remaining 09:52:39
    IdleTime granted 00:10:00 (10 min), remaining 00:09:24
    Flags sBdmg-T-, Identification CCA7F408.1
    Tunnel0 src 81.81.81.81 dest 2.2.2.200 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit not set
```

OM Metrics for 3GPP2 / WiMAX Bindings

This feature returns peak value for MaxActiveBindings, MaxActive3GPP2Bindings and MaxActiveWimaxBindings when queried for OIDs for the previous interval.

Cisco HA Release 5.1 introduces two timers to handle the OM Metric feature. One of the timers supports the interval starting at the top/bottom according to NTP time. The second timer calculates the OM metrics. The first timer starts when the router boots up, or when the command is modified. The second timer starts when the first timer expires, and this timer expires based on a configured value.

By default this feature is enabled with a default interval of 30 minutes. The default configuration is not displayed in the running-configuration.

Note Redundancy is not supported for the OM-metrics feature.

Configuring OM Metrics

To configure the interval for this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# om-metric-interval {15 | 30 | 60 }`	This is a sub-command that is available under sub-menu of the **ip mobile options** command.

Here is sample output to help verify the configuration:

Metric counters such as number of 3gpp2 bindings, number of Wimax bindings, etc., are displayed under **show ip mobile binding summary**.

```
router#sh ip mob binding summary
Mobility Binding List:
Total 1
3gpp2 Bindings 1
Wimax Bindings 0
```

The new metric values are displayed under a new command.

```
router#show ip mobile options ommetrics
OM Metric Statistics:

 Peak Active bindings in the elapsed (previous) interval 0
 Peak Active 3GPP2 binding in the elapsed (previous) interval 0
 Peak Active Wimax binding in the elapsed (previous) interval 0
 Elapsed configured interval size is 15 minutes
```

Additionally, the following new debug statements are printed when **debug ip mobile** is enabled:

```
%IPMOBILE-6-OMMETRICS_TIMER_INFO: OM Metric Interval Timer will be started after 1170577
milliseconds.
MobileIP:  OM Metric Sleep Timer is Started
MobileIP:  OM Metric Sleep Timer is Stoped
MobileIP:  OM Metrics Interval Timer is Started for 900005 milliseconds
MobileIP:  OM Metrics Interval Timer is Expired
MobileIP:  OM Metrics Interval Timer is Stoped
MobileIP:  System clock has been updated,
                    So Om Metric Timers will restart
%IPMOBILE-4-OMMETRICS_TIMER_WARNING: Clock skew is more, So Om metric timers will restarts
 metrics interval time is 900000.
 deltaOffset is 39599997.
 currentSystemClock is 3599997.
 nextSystemClock is 50400000.
```

Single IDB for MIP/UDP Tunnels

MIP/UDP RFC 3519 requirements dictate that each MIP/UDP CCoA binding to the MN requires a separate MIP/UDP tunnel. In HA Release 5.0, the HA utilized a hardware/software Interface Descriptor Block (IDB) for each tunnel. Since the system can support a maximum of 16K hardware IDBs, the maximum number of MIP/UDP CCoA bindings is limited to 16K.

Cisco HA Release 5.1 can support hundreds of thousands of MIP/UDP CCoA bindings. In order to support this requirement, we utilize a Single IDB for all types of tunnels.

The Single IDB, or tunnel scalability feature, supports MIP/UDP tunnels only. However, the functionality of other types of tunnels (such as IP/IP and GRE/IP) is not affected.

As part of this feature support:

- Tunnel APIs are modified as required so that other types of tunnels such as IP/IP, GRE/IP, etc., are not affected and remain functional.
- The supported CPS rate for MIP/UDP tunnels (either CoA or CCoA) remains the same as HA 5.0.
- The supported data throughput rates for MIP/UDP tunnels (either CoA or CCoA) remains the same as HA Release 5.0
- The maximum number of supported MIP/UDP tunnels on a 1GB SAMI card will be 80,000. To achieve this number I/O Memory has to be increased from 64MB to 128MB.

Configuring the SAMI for Single IDB

Note To configure the I/O Memory from 64MB to 128MB, issue the **memory-size iomem 128** command, and reboot the card after changing I/O Memory.

Verifying the Configuration

There are no new configuration tasks to implement this feature. The following commands are modified to verify that the Single IDB feature is functional.

show ip mobile tunnel summary command output is modified as follows:

```
#show ip mob tunnel sum
Mobile IP tunnels summary:
   One IDB used per tunnel for IP/IP, GRE/IP tunnels
   Single IDB used for MIP/UDP tunnels

   Total mobile ip tunnels 2
```

show ip mobile tunnel command output is slightly modified for MIP/UDP tunnels only. The two changes that are applicable to MIP/UDP tunnels are:

- The tunnel number for all MIP/UDP tunnels will be same because all MIP/UDP tunnels are utilizing the single IDB feature.
- Tunnel stats are stored in IDB data structure. Since we have a single IDB for all MIP/UDP tunnels, individual tunnel counters are be displayed for MIP/UDP tunnels. However, aggregate-statistics for all tunnels is displayed using a new show command, **show ip mobile tunnel mip-udp aggregate-statistics**.

The output of the IP/IP and GRE/IP tunnels will remain same.

```
router#show ip mob tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1244
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1245
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
```

The **show ip mobile tunnel mip-udp aggregate-statistics** output will display as follows:

```
router#show ip mob tunnel mip-udp aggregate-statistics
Tunnel0 Aggregate Counters:
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    300 packets input, 45600 bytes, 0 drops
    300 packets output, 39600 bytes
```

In the **show ip mobile traffic** output, the number of keepalives received and sent on all tunnels is displayed under this existing show command. New lines are highlighted below:

```
router#show ip mob traffic
IP Mobility traffic:
```

```
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 22961, denied 0, ignored 0, dropped 0, replied 22961
    Register requests accepted 22961, No simultaneous bindings 0
  . . .
  . . .
  . . .
MIP/UDP Tunnel:
    Number of Keepalives received (on all tunnels) 13809
    Number of Keepalives sent (on all tunnels) 13809
```

GRE Key CVSE in Non-VRF Environment

MIPv4 supports GRE/IP tunneling without using GRE keys. The GRE CVSE extension allows an FA to request GRE tunneling, and also allows both the HA and FA to exchange the upstream and downstream GRE keys for GRE/IP tunnels.

Here is a call flow that illustrates how this feature works:

1. The FA generates the GRE key, adds the GRE key extension to the RRQ, and forwards it to the HA.
2. The HA receives the initial registration RRQ and parses the GRE key extension. If a poorly formed GRE key extension is received, the HA sends RRP with “unknown CVSE”.If the registration is accepted, the HA creates a binding and stores the GRE key provided by FA inside the binding. If a reverse tunnel is requested, the HA also creates a unique GRE key (HA generates a random number and compares it against the already allocated GRE keys for uniqueness), and returns an RRP with the GRE key extension. The HA does not check for duplication in keys provided by FA.
3. When reverse tunnel is enabled, the FA tunnels the upstream traffic (i.e., from the MN to the CN) to the HA and when the FA tunnels a packet to the HA, it adds the GRE key (which was provided by HA in RRP). When the HA receives a packet with the source and destination IP addresses matching its tunnel, it also matches the GRE key in the encapsulated packet.
4. For downstream traffic (i.e., from the CN to the MN), the packet from the CN reaches the HA and the HA has a routing entry for the MN pointing to the HA-FA tunnel. The binding for the MN is looked up and the GRE key stored in the binding is used to encapsulate the packet and tunneled to the FA.
5. If the HA receives a re-registration RRQ, it parses the GRE key extension. If the re-registration is accepted, the HA updates the binding with the downstream key received in the re-registration RRQ and responds back an RRP with previously generated upstream key for use by the FA.
6. If HA receives a valid de-registration RRQ with a GRE key extension (if present) the HA responds back an RRP containing the previously generated upstream GRE key.

Redundancy Considerations:

Redundancy is supported for GRE CVSE feature.

Other Considerations

If an incoming RRQ (initial/renew/de-registration) has a GRE key value of zero (0),

- The HA will generate GRE key, even when Reverse tunneling bit (T) is not set.
- When T bit is set in the RRQ, the key generated by HA is used for both the directions.

- Irrespective of G bit status in the RRQ, the tunnel mode will be set to GRE when GRE CVSE extension is present in RRQ.

Configuring GRE Key in a Non-VRF Environment

To configure the Cisco Mobile Wireless HA to identify data streams for the individual sessions based on the GRE key in GRE tunnels, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent options`	Enables the configuration of IP Mobile Home Agent options, and enters IP Mobile Home Agent option configuration submode.
Step 2	`Router(config-ipmobile-ha-options)#cvse gre-key`	Enables GRE tunneling with GRE keys from CVSE. You cannot enable or disable this command if there are active bindings in the system. The default behavior is to not parse the GRE key from CVSE.

Support for RFC 4917

RFC 4917 specifies the Message String Extension appended to Registration Replies or Registration Revocation messages that are sent to the terminal to provide users with a displayable notification from the network. The text in the extension can be obtained from the AAA server through the RADIUS Reply-Message attribute that is carried in Access-Accept, Access-Reject, or Disconnect (RFC 3576) messages. The RADIUS Change of Authorization does not cause Registration Reply or Registration Revocation messages to be sent. Thus, this message is not supported for the Mobile IP extension.

Debug output that displays mobile registration messages includes registration reply and revocation messages.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent message-string`	Enables or disables the delivery of the text from the AAA server to the user.

Here is a sample configuration for the Message String extension:

HA Config

```
ip mobile home-agent template Tunnel10 address 10.10.10.188
ip mobile home-agent template Tunnel10 address 10.10.10.203
ip mobile home-agent template Tunnel10 address 10.10.10.179
ip mobile home-agent binding-overwrite
ip mobile home-agent message-string
ip mobile home-agent accounting ha-acct
ip mobile virtual-network 2.0.0.0 255.0.0.0
ip mobile host nai @aricent.com address pool local mip-pool-1 virtual
network 2.0.0.0 255.0.0.0 aaa load-sa lifetime 3600
ip mobile secure mn-aaa spi 101 algorithm md5 mode ppp-chap-style
```

RADIUS Config

```
simulator radius subscriber 123
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
```

```
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  attribute 18 string “Welcome TO Cisco”

simulator radius subscriber 124
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  reply-message RFC4917 “HA-CHAP Failed”
```