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:

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.

Limitations

When you use PMIP with Session Redundancy and you choose the “msec” option for the timestamp (**ip mobile foreign-service revocation timeout** 5 **retransmit** 4 **timestamp msec**), and opened a PMIP flow with PDSN SR setup. The **cdma redundancy** debug output shows the “revocation timestamp” value on the active and standby PDSNs are the same.

If you perform a switchover, the standby PDSN takes over as active. If you try to close the PMIP flow, the revocation message sent from the PDSN to the HA is ignored on HA because the timestamp is mismatched. Thus, after several re-tries, the PDSN deletes the revocation entry pending for Ack, and the binding on HA is not deleted.

This limitation is not related to synching the attribute, but the uptime of the router, as the **msec** option puts the uptime in the timestamp field and uptime of standby router is expected to be lower. If you utilize the default **seconds** based option (which puts a timestamp in UTC), this may not be an issue. Additionally, **msec** has another issue of wrap-around in 49+ days, so it cannot be used in an always-on setup.

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 RRQ from 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).

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
- Signalling 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.

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:

```
SAMI-PPC3-SLOT4#sh 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.

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 16-1 identifies the WiMAX AAA Authorization attributes for the Home Agent.

Table 16-1 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

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 31323334353637383930313233343536373839 30
```

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 16-2 identifies the WiMAX AAA Accounting Attributes for the Cisco HA:

Table 16-2 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
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
```

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 16-3 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.

Table 16-3 AAA Authentication and Accounting Attributes on the AAA Server (continued)

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
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
```

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”
```