CHAPTER 15

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.

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.

Note 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).

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)
```

Support for Max Bindings

The following functionality is available to support Max bindings:

- Command for the maximum number of bindings allowed.
- Raise SNMP alert to the NM when the number of bindings reaches the maximum.

Once you configure the maximum number of bindings, the system restricts the number of bindings to the specified value. Once the system accepts to maximum number of bindings, it rejects all incoming registration requests, and raises an SNMP alert to the NM. Once the number of bindings falls back below the threshold value, the alert is cleared.

The lower threshold value for clear the SNMP trap is 90% of max binding value. If the number of bindings is reduced to 90% of the max bindings, the HA will clear the SNMP trap.

You should throttle the trap to avoid flooding trap activity. To ensure this, the HA sends the notification once when the number of bindings exceeds the maximum bindings, and it will be not be generated again until the number of bindings falls back to threshold and reaches maximum bindings.

Perform the following task to configure support for max bindings:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent max-binding` *max-binding-value*	Enables the maximum dfp weight allowed on HA. By default, the max dfp weight value is 24.

This feature is disabled by default, and the maximum number of bindings that can be configured on the HA depends on the platform.

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*	Enables the maximum dfp weight allowed on HA. By default, the max dfp weight value is 24.
Step 2	`Router(config)# ip mobile home-agent max-cps` *max-cps-value*	Enables the maximum cps allowed on HA. By default, the max cps value is 160cps with accounting support.

MIP/LAC (PPP Regeneration) Support

This feature allows the HA to map a MIP call to a PPP session in a VPDN tunnel based on the configuration.

Many corporate networks and L2TP Network Servers (LNSs) have existing Virtual Private Dialup Network (VPDN) connections to the Internet and Internet Service Providers (ISPs) to handle incoming dialup connections. These connection methods ensure security over public networks. Most of these VPDN connections come through L2TP tunnels by encapsulating incoming packets with PPP inside the L2TP tunnel.

Using HA technology, user data traffic that originates from a Mobile Node (MN) that is connected to Foreign Agent (FA) can be delivered to corporate networks through the Home Agent (HA). Additionally, the HA can deliver data traffic to the LNSes in a conventional dialup scenario.

The MN connects to the HA through a FA using a regular MIP tunnel. When enabled, the HA can setup an L2TP tunnel to a corporate LNS and map a MIP session to a PPP session within the L2TP tunnel. Now, an MN can be connected back to the corporate network by utilizing the available infrastructure.

Note The ability of the HA to transport MN data traffic to a corporate LNS is called the MIP-LAC feature. It means that the HA terminates a MIP session, and additionally, regenerates a new PPP session for a MIP session within L2TP tunnel.

The following call flow illustrates the sequence of events from the time the MN sends a RRQ to the time it receives a RRP reply when MIP-LAC functionality is enabled for the MIP session.

Note The following call flow describes the most common scenario (obtaining VPDN parameters from AAA), and does not include all possible scenarios.

The events are described as follows:

1. The MN receives Mobile IP advertisement with FA-CHAP challenge from the FA.
2. The MN sends RRQ with FA-CHAP extension to the FA.
3. The FA sends an Access-Request to the visiting AAA (V.AAA) to authenticate the MN. The VAAA may further contact the Home AAA (H/SP.AAA) for MN authentication.
4. When the FA receives the Access-Accept from the AAA server, it forwards a RRQ (originally sent by the MN) to the HA.
5. The HA authenticates this message with the help of the HAAA server. The HA sends an Access-Request to the AAA and receives an Access-Accept from the AAA.

6. The HA scans the attributes received in the Access-Accept message. If the VPDN tunnel setup parameters are identified in the message, the HA will initiate a VPDN tunnel (in this instance, an L2TP tunnel) to LNS.
7. As part of L2TP tunnel setup, tunnel parameters are negotiated during LCP and IPCP phases of PPP.
8. After completion of the L2TP tunnel setup, an RRP is sent to the MN through the FA.

After the L2TP tunnel is setup between the HA and LNS, the HA will act as an agent; it transports mobile IP data traffic into the L2TP tunnel, and vice versa.

When MIP-LAC is enabled for user(s) and HA does not go to AAA for authentication / authorization, local configuration will be checked for VPDN parameters.

Configuring MIP LAC

Here are the essential steps to enable a VPDN configuration locally:

	Command	Purpose

Step 1	`Router(config)#ip mobile host nai @xyz.com address pool ?`
	`  dhcp-pool  Use local DHCP pools`
	`  dhcp-proxy-client  Use DHCP proxy client feature`
	`  local  Use local address pool`
	`  vpdn-tunnel  Use VPDN tunnel feature`
	
	`Router(config)#ip mobile host nai @xyz.com address pool vpdn-tunnel ?`
	`  interface  Home link is on this interface`
	`  virtual-network  Home link is on this virtual network`
		Indicates address pool type as **vpdn-tunnel** (this is a new option).
		
		For an existing **ip mobile host** command, a new **vpdn-tunnel** option is added to indicate that the address for mobile IP client needs to be obtained from LNS server using MIP-LAC feature.

Step 2	`router# ip mobile realm` *`@xyz.com`* `vrf` *`vrf-name`*
	`ha-addr` *`ip-address`* `[aaa-group [accounting`
	`aaa-acct-group` `|` `authentication` *`aaa-auth-group`*`]]`
	`[dns dynamic-update method` *`word`*`] [dns server` *`primary dns server address secondary dns server address`*
	`[assign]] [hotline] | [`**`vpdn-tunnel`**` virtual-template`
	`number` `[setup-time` *`number`*`]]`
		Enable MIP-LAC functionality for a user.

For an existing **ip mobile realm** command, a new option **vpdn-tunnel virtual-template** *number* is added to enable MIP-LAC feature for specific user(s). Here, **setup-time** for **vpdn-tunnel** configuration is optional. The range of values for **setup-time** is from 5 secs to 300 secs. The default value for setup-time will be 60 seconds. The default value will be taken in to consideration, when you do not specify the **setup-time** option explicitly.

Configured **setup-time** is the maximum tolerance time, starting from the creation of the PPP IDB within which a regenerated PPP session has to come fully up. If this period of time has elapsed and the L2TP tunnel is not up yet, Mobile IP module proceeds to tear down this session's L2TP session, PPP IDB and mobile binding. Also, please note that *number* option of **tunnel vtemplate** *number* must match the number configured in the corresponding **interface virtual-template** command.

Step 3	`Router(config)# interface virtual-template number`
	`Router(config-if)# ip address negotiated`
	`Router(config-if)# no peer neighbor-route`
	`Router(config-if)# encapsulation ppp`
		Configures the PPP virtual template interface on the HA.
		Note The **interface virtual-template** *number* must match the number configured in the corresponding **vpdn-tunnel vtemplate** command.

Also, **ip address negotiated** and **no peer neighbor-route** must be configured for **virtual-template**. Cisco IOS software automatically creates neighbor routes by default; that is, it automatically sets up a route to the peer address on a point-to-point interface (in other words, the HA interface connecting LNS server) when the PPP IPCP negotiation is completed. To disable this default behavior, use the **no peer neighbor-route** command. The no authentication method should be configured on this interface. Configuring an authentication method indicates that HA/LAC authenticates LNS, which is not required. LNS authenticates HA/LAC but not HA/LAC authenticates LNS.

Step 4	`aaa new-model`
	`aaa authentication ppp default local`
	`!`
	`username lac password 7 192840824D76`
	`username lns password 7 320985235A35`
		Adds AAA parameters for locally configured LAC.
		These commands indicate to the HA to use local configuration to complete tunnel authentication.

Step 5	`vpdn enable` `vpdn search-order domain`	Enables VPDN and VPDN search order. These commands need to be configured to enable VPDN functionality on the HA. The **vpdn search-order domain** command indicates to the HA how to search for VPDN configuration based on domain match. With this command, the **domain** of the connecting MN is looked at for a match in VPDN groups.

Step 6	`vpdn-group 1`
	` request-dialin`
	`  protocol l2tp`
	`  domain xyz.com`
	` initiate-to ip 1.1.1.1`
	` local name lac`
		Configures VPDN tunnel authorization attributes locally by creating a new group and associates the required VPDN parameters to the group.
		The **domain** configured for **vpdn-group** should be same as **realm** configured for **ip mobile realm** with out “@” character. If configured, the VPDN parameters are insufficient to set up a tunnel, then the configuration will be considered as invalid, and the tunnel will be aborted.

Step 7	`vpdn-group 1`
	` request-dialin`
	`  protocol l2tp`
	`  domain xyz.com`
	` initiate-to ip 1.1.1.1`
	` initiate-to ip 2.2.2.2`
	` initiate-to ip 3.3.3.3`
	` local name lac`
		Configures LNS load balancing based on local configuration
		
		Multiple instances of the **initiate-to ip** command in VPDN group configuration mode configure the session load balancing feature locally.

Step 8	`ip vrf moip-vrf-comp4`
	` rd 100:4`
	`!`
	`ip mobile realm @xyz.com vrf moip-vrf-comp4 ha-addr 13.1.1.119`
		Configures VRF based on local configuration.
		
		When VRFs are configured on the HA, and a specific MIP-LAC tunnel is for a specific VRF instance of the HA, these commands need to be configured on the HA.

When MIP-LAC is enabled for user(s) and VPDN parameters are received from AAA in Access-Accept message, then the VPDN configuration downloaded from the AAA server is utilized. VPDN parameters downloaded from AAA will always take higher precedence. If downloaded VPDN parameters are insufficient to set up a tunnel, then the configuration will be considered as invalid and tunnel will be aborted.

Step 9	`radius host 6.6.6.6 auth-port 1645 acct-port 1646` `radius-server key cisco`	Configures RADIUS server to download VPDN attributes.

The **domain** of VPDN parameters should be same as **realm** configured for **ip mobile realm** without the "@' character. If configured VPDN parameters are insufficient to setup tunnel, then, configuration will be considered as invalid and tunnel will be aborted.

LNS Load Balancing Based on AAA Server Configuration

It is possible to configure the LACs to perform round robin load sharing across 2 or more LNSs. To do this, simply define more than one IP address (or DNS hostname) for the destination LNSs, and comma delimits them. For example, you could modify the above example to support two additional LNSs:

```
Cisco-avpair = "vpdn:ip-addresses=1.1.1.1, 2.2.2.2, 3.3.3.3"
```

This LNS load balancing functionality already exists in IOS. While bringing up a MIP-LAC tunnel, if more than one LNS address is returned by the AAA server, an LNS address is chosen based on round-robin algorithm currently implemented in IOS.

Configuration on LNS

Note This sample LNS configuration accepts dial-in connections from HA/LAC. However, explanations are beyond the scope of this document.

```
version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
hostname lns
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authentication ppp vpdn radius
aaa authorization network default radius
```

```
aaa accounting network default start-stop radius
!
username lac password 7 104D000A0618
username lns password 7 060506324F41
!
vpdn enable
!
vpdn-group 1
 accept dialin
 protocol l2tp
 virtual-template 1
 local name lns
 l2tp tunnel password 7 02347324D3
 source-ip 4.4.4.4
!
async-bootp dns-server 1.1.1.1 2.2.2.2
async-bootp nbns-server 8.8.8.8 9.9.9.9
!
!
interface FastEthernet0/0
ip address 172.22.66.25 255.255.255.192
no ip directed-broadcast
no ip mroute-cache
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
peer default ip address pool default
ppp authentication chap vpdn
ppp multilink
!
ip local pool default 10.1.1.1 10.1.1.16
...
!
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
end
```

Configuration on AAA

The following configuration should be place into the users' file on the corresponding RADIUS server for domain "cisco.com"

```
    Password = "cisco",
    Service-Type = Outbound-User,
    Cisco-avpair = "vpdn:tunnel-id=nas",
    Cisco-avpair = "vpdn:tunnel-type=l2tp",
    Cisco-avpair = "vpdn:ip-addresses=1.1.1.1",
    Cisco-avpair = "vpdn:l2tp-tunnel-password=lab"
    Cisco-avpair = "outbound:send-auth=2"
    Cisco-avpair = "outbound:send-name=dgudimet"
    Cisco-avpair = "outbound:send-secret=password"
    Cisco-avpair = "mobileip-vrf-ha-addr=13.1.1.121"
    Cisco-avpair = "ip:ip-vrf#0=moip-vrf-comp4"
```

These parameters are downloaded to the HA/LAC as part of Access-Accept message from AAA server.

VRF Configuration Based on AAA Server Configuration

When VRFs are configured on the HA and a specific MIP-LAC tunnel is for a specific VRF instance of the HA, the following commands need to be configured:

```
ip vrf moip-vrf-comp4
 rd 100:4
```

And, the following configuration needs to be put into the users file on the corresponding RADIUS server for domain *cisco.com*.

```
Cisco-avpair = "mobileip-vrf-ha-addr=13.1.1.121"
Cisco-avpair = "ip:ip-vrf#0=moip-vrf-comp4"
```

Verifying the Configuration

Perform the following tasks to verify the MIP LAC configuration:

Step 1	`router#` **`show ip mobile binding`**	Displays additional information about the L2TP tunnel when a MIP-LAC session is established for a specific IP mobile session. The **setup-time** indicates the maximum setup time taken to establish an L2TP session. This command also displays the number of active L2TP/PPP regenerated sessions. The total number of sessions is inclusive of the total number of MIP-LAC sessions (VPDN tunneled).
Step 2	`router#` **`ip mobile binding summary`**	Displays the total number of active L2TP/PPP regenerated sessions. The total number of sessions is inclusive of the total number of MIP-LAC sessions (VPDN tunneled).
Step 3	`router#` **`show ip mobile traffic`**	Displays additional counters related to MIP-LAC.

Here is an example:

```
Router# show ip mobile binding
Mobility Binding List:
Total 15000
Total VPDN Tunneled 20
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
    VPDN Tunnel (setup-time 30)
    Acct-Session-Id: 1677265
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

Here is an example of the **ip mobile binding summary** command:

```
ha#show ip mobile binding summary
Mobility Binding List:
Total 15000
Total VPDN Tunneled 20
```

Here is an example of the **show ip mobile traffic** command:

```
HA#show ip mobile traffic
IP Mobility traffic:
Time since last cleared: 00:05:59
```

```
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 2, denied 1, ignored 0, dropped 0, replied 2
    Register requests accepted 1, No simultaneous bindings 0
    Register requests rcvd initial 2, re-register 0, de-register 0
    Register requests accepted initial 1, re-register 0, de-register 0
    Register requests replied 2, de-register 0
    Register requests denied initial 1, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 1, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 0, sent 1 total 1 fail 0
    Binding Update acks received 1 sent 0
    Binding info requests received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Binding Delete Req received 0, sent 0 total 0 fail 0
    Binding Delete acks received 0 sent 0
    Binding Sync Req received 0, sent 0 total 0 fail 0
    Binding Sync acks received 0 sent 0
    Gratuitous 3, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
    Total incoming registration requests using NAT detect 0
    Total VPDN Tunnel sessions attempted: 1 success: 1 fail: 0 pending: 0
                                PPP IDBs: 1 no resource: 0 deleted: 0
Foreign Agent Registrations:
    Register requests rcvd 0, valid 0, forwarded 0, denied 0, ignored 0
    Register requests valid initial 0, re-register 0, de-register 0
    Register requests forwarded initial 0, re-register 0, de-register 0
    Register requests denied initial 0, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0,  de-register 0
    Register replies rcvd 0, forwarded 0, bad 0, ignored 0
    Register replies rcvd initial 0, re-register 0, de-register 0
    Register replies forwarded initial 0, re-register 0, de-register 0
    Registration Errors:
      Unspecified 0, HA unreachable 0
      Administrative prohibited 0, No resource 0
      Bad lifetime 0, Bad request form 0
      Unavailable encapsulation 0
      Unavailable reverse tunnel 0, Reverse tunnel mandatory 0
      Authentication failed MN 0, HA 0
      Received challenge/gen. authentication extension, feature not enabled 0
      Unknown challenge 0, Missing challenge 0, Stale challenge 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
```

The new MIP-LAC feature related counters added are:

```
Total VPDN Tunnel sessions attempted: 34 success: 33 fail: 1 pending: 0
                           PPP IDBs: 34 no resource: 6 deleted: 34
```

Here is an explanation for these new counters:

- **attempted** - total number of MIP-LAC sessions attempted as a result of matched mobile ip registration requests.
- **success** - total number of successful MIP-LAC sessions out of all attempts.
- **fail** - total number of failed MIP-LAC sessions out of all attempts.
- **pending** - total number of MIP-LAC sessions that are pending (in-progress state) out of all attempts.
- **PPP IDBs** - total number of PPP IDBs that are created in order to bring up MIP-LAC sessions.
- **No resource** - total number of sessions that failed to complete due to resource crunch (for example, unavailability of IP addresses, unavailability of memory, etc.).
- **Deleted** - total number of sessions brought down after successful establishment of the session (either manually by the administrator, or due to error).

Restrictions

Please note following software configuration restrictions for this feature:

- If VRF is configured on an interface that HA connects to the LNS, MIP-LAC feature will not work as it is supposed to be.

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 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: 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.
- WiMAX Capability: when this attribute is present in the Access-Request message sent to the HAAA, it may also be present in the received Access-Accept message. When present in an Access-Accept message received at the HA, it can contain only the Accounting Capabilities sub-TLV, which indicates the accounting capabilities selected by the server for the session. It is expected that the accounting capabilities returned by the HAAA in the Access-Accept match the value specified by the HA in the Access-Request. The HA currently does not process the WiMAX Capability VSA received in the Access-Request in any way, and performs no verification if the accounting capabilities match.
- HA-IP-MIP4: will be included in all Access-Request messages from the HA. For existing bindings (i.e., Access-Requests corresponding to re-registration and deletion), its value is set to the Home Agent address for the binding. In Access-Requests for new bindings, the value of this attribute will be set to HA IP address configured using the **ip mobile home-agent address** or the **ip mobile home agent redundancy** commands.
- RRQ-HA-IP: the HA includes this attribute in an Access-Request message only 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 15-1 identifies the WiMAX AAA Authorization attributes for the Home Agent.

Table 15-1 WiMAX AAA Authorization Attributes

Attribute Name	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject	Supported in HA 4.0
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

Table 15-1 WiMAX AAA Authorization Attributes (continued)

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
RRQ-MN-HA-SPI	26/20	The SPI associated with the RRQ-MN-HA-KEY.	1	0	1	0	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

If the Access-Request from the HA contains the HA-RK-Key-Request VSA with the value set to **1**, the HAA will return the HA_RK-KEY, HA-RK-SPI and HA_RK-Lifetime attributes in the Access-Accept. If one of these attributes is present, then all must be present. If not the HA discards the Access-Accept. This attribute is not included in any of the Accounting (Start/Stop/Interim) messages.

The HAAA creates a random 160 bit HA-RK key for each HA. 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.

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 = IP address expressed as a 32-bit value of the HA as seen from the FA and as reported in the Mobile messages

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 along with the SPI is used to validate this extension.

HMAC-SHA1 generates a 20 byte output. The current HA implementation only supports HMAC and HMAC-MD5 algorithms for the FHAE, which only require a 16 byte key. HA 4.0 uses the first 16 bytes of the HMAC-SHA1 output as the key for the FHAE verification.

The HA includes the SPI received in the MHAE as the value of the MN-HA-MIP4-SPI attribute in the Access-Request. The value of the MN-HA-MIP4-KEY attribute downloaded from the AAA corresponding to the SPI value in the MN-HA-MIP4-SPI attribute is used to verify the MHAE in the Mobile IP RRQ. It is also possible to configure the SPI and the key to be used for MHAE verification locally using the **ip mobile secure host** command.

If the MobileIP RRQ received by the HA contains the FHAE extension, the HA includes the HA-RK-Key-Requested attribute in the Access-Request to the HAAA 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 HA uses the value of the HA-RK-KEY attribute downloaded from the AAA corresponding to the SPI value in the HA-RK-SPI attribute to generate the FA-HA Key to be used for FHAE verification. The FA-HA Key is generated from the HA-RK-KEY as specified in the WiMAX Forum Stage 3 Specifications (R1.0.0, Section 4.3.5.1). It is also possible to configure the SPI and the key to be used for FHAE verification locally using the **ip mobile secure foreign-agent** command.

When WiMAX AAA attribute functionality is enabled through CLI, the HA will include WiMAX AAA attributes in accounting start/stop messages that are sent to the HAAA server.

HA-AAA Accounting Attributes Support for WiMAX

This existing 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 15-2 identifies the WiMAX AAA Accounting Attributes for the Cisco HA:

Table 15-2 WiMAX AAA Accounting Attributes

Name	Type	Description	Start	Int	Stop
Session-Continue	26/21	True indicates that the stop is immediately followed by a start. If the attribute is missing or FALSE it means that this is the final stop.	0	0	0-1
Beginning of Session	26/22	True: a new flow is starting. False or missing, this is a continuation of a previous flow.	0-1	0	0
Hotline-Indicator	26/24	Indicates that the flow is hotlined	0-1	0-1	0-1
Calling-Station-Id	31	The MAC address of the MS	1	1	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
Control-Packets-In	26/31	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.	0	0-1	0-1
Acct-Input-Packets-Gigaword	26/48	Incremented when attribute 47 overflows	0	0-1	0-1
Acct-Output-Packets-Gigaword	26/49	Incremented when attribute 48 overflows	0	0-1	0-1
Control Octets In	26/32	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.	0	0-1	0-1
Control Packets Out	26/33	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1	0-1
Control Octets Out	26/34	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1	0-1

Configuring WiMAX Support

Perform the following tasks to enable the WiMAX AAA support on the HA:

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 (26/2) • RRQ-HA-IP (26/18) • MN-HA-MIP4-SPI (26/11) • RRQ-MN-HA-SPI (26/20)
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 (26/2) • 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
```

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 15-3 AAA Authentication and Accounting Attributes on the AAA Server

RSIM 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
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.

Table 15-3 AAA Authentication and Accounting Attributes on the AAA Server

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.
attribute 20 *spi hex value* range of hex value- 100-FFFFFFFF	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.

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
```