CHAPTER 15

Monitoring User Traffic

This chapter discusses how to monitor upstream and downstream user traffic using the Hotlining feature, and provides details on how to configure the feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

Hot-lining

Hot-Lining provides a wireless operator with the capability to efficiently address issues with users that would otherwise be unauthorized to access packet data services. When a problem occurs such that a user may no longer be authorized to use the packet data service, a wireless operator using this feature may Hot-Line the user, and upon the successful resolution of the problem, return the user's packet data services to normal once the hot-lined condition is resolved. When a user is Hot-Lined, their packet data service is redirected to a Hot-Line Application which may notify (if feasible) the user of the reason(s) that they have been Hot-Lined and offers them means to address the reasons for Hot-Lining, meanwhile blocking access to normal packet data services.

HA support Profile based hot-lining with Filter/IPRedirection/HTTPRedirection by using Active and New session hot-lining for 3gpp2/wimax environment subscribers.

HA Release 5.1 does not deal with Rule based hot-lining for both 3gpp2/Wimax environment with Active and New session hotlining. HA5.1 does deal with IS835-D and NWG 1.3.1 Stage 2 standards for Hot-lining support.

In HA Release 5.1, there is one style of hot-lining is supported on HA which will be triggered by the HAAA to indicate that a user be hot-lined:

- In profile-based hot-lining, IP or HTTP, or both redirection rules are configured under a profile on the HA. The HA performs hot-lining after it receives the Filter-Id from the home AAA in either an Access-Accept, or a COA. The HA sends the hot-line capability parameter in the Access-Request message.

Note The Filter-ID matches one of the profiles on the HA.

Additional Hot-Lining Features

On the Home Agent, the hot-lining policy is applied only when the policy is downloaded during HA CHAP. The Home Agent will reject the RRQ if Reverse-Tunnel is not requested by the user and hot lining policy is downloaded for the user.

Note There is no MIB support planned for this feature.

The hot-lining feature enables you to monitor upstream user traffic using two different scenarios-active and new session. When hot-lining is active for a particular user, the upstream IP packets from the mobile are re-directed to the Re-direct server that is configured for this particular realm. Re-direction is achieved by changing the IP packet destination address to the Re-direct server address. The only mandatory attribute supported in the Change of Authorization (CoA) message from the HAAA is the User-Name attribute to identify the particular user on the Home Agent. Optionally, IP address can also be sent in the CoA message to identify the particular binding for a particular user.

New Session Hot-Lining

Here is the process by which a new session is hot-lined.

Step 1 The HAAA receives a signal from the hot-lining application to hot-line a user's packet data service.

Step 2 The HAAA records this information in its user profile store. If the user is not active, the HAAA waits until the user initiates the packet data service, which causes the user to be hot-lined immediately. Meanwhile, it is possible for the hot-line application to change the user's hot-line status back to normal, in which case the HAAA updates the user profile, and stores it accordingly.

Step 3 When the user who is to be hot-lined initiates a packet data session, a RADIUS access-request is received by the HAAA that indicates the hot-line capability of the HA.

Step 4 In the HAAA, the local policies and received hot-line capability parameter is used to determine which HA receives the hot-lining VSAs. The HAAA signals the hot-lining device of the user's hot-line status by sending hot-lining VSA(s) in the RADIUS Access Accept message. The HAAA may include the hot-line accounting indication VSA in the RADIUS access-accept message.

Step 5 If accounting is enabled on the HA, the HA generates a RADIUS accounting-request (start) packet and includes the hot-line accounting indication VSA if it was received in the RADIUS access-accept message. If the HA is unable to honor the hot-lining VSA(s) received in the RADIUS access-accept packet, it treats the RADIUS access-accept packet as a RADIUS access-reject packet, and terminates session setup.

Step 6 Once a hot-line session starts, traffic is blocked and/or directed to the hot-line application.

Active Session Hot-Lining

The following procedure lists the events for active session Hot-lining:

Step 1 The user is currently engaged in a packet data session that is not hot-lined.

Step 2 The HAAA starts the active session hot-lining procedure when it receives a hot-line signal from the hot-line application for a user that has already started a packet data session.

Step 3 The HAAA stores the hot-line state of the user in the user's profile.

Step 4 In the HAAA, the local policies and received hot-line capability is used to determine which HA receives hot-lining VSAs. The HAAA signals the HA of the user's hot-line status by sending hot-lining VSA(s) or RADIUS filter-id (11) attribute in the RADIUS change of authorization (COA) message. The HAAA may include the hot-line accounting indication VSA in the RADIUS COA message for 3gpp2 environment users.

Step 5 If the HA can honor the request then it responds with a COA ACK packet. If the HA cannot honor the hot-lining request, then the HA responds with a COA NAK message. Based on local policy, upon receiving a COA NAK message with error-cause (101) indicating "Administratively Prohibited (501)", the HAAA may either retry sending the hot-lining signal to the HA, or send a RADIUS disconnect-request message to the HA, or to another device to instruct it to drop the session.

Step 6 An HA capable of generating accounting packets (if accounting is enabled) also generates a RADIUS accounting-request (stop) message to close the current accounting session. The release indicator (F13) is set to 14 (hot-line status changed) for only 3gpp2 environment users.

Step 7 An HA capable of generating accounting packets also generates a RADIUS accounting-request (start) message that includes the hot-line accounting indication VSA received in the COA packet.

Step 8 The hot-lining device then immediately invokes the hot-lining profiles as specified in the COA packet.

Step 9 Once the user has been hot-lined, the hot-line application might notify the user of their hot-lined state, and will interact with the user to rectify the issue that caused the hot-lining. If the hot-lining application is not satisfied with the results, it may maintain the hot-lining status of the user, or it may terminate the users session. If the problem has been rectified the hot-lining application will return the user's session back to a normal mode.

Step 10 The hot-line application will indicate the return to normal status to the HAAA. The interaction of the hot-line application with the user is beyond the scope of this document.

Step 11 The HAAA updates the user's profile.

Step 12 If the session is active, the HAAA sends a COA packet to the HA that is currently applying the hot-line rule. This may not be the same device that initially implemented the hot-line state for the session (a handoff may have happened). If the received notification, of Step 9 indicated session termination from the hot-line application, the HAAA records the termination status of the user in the user's policy store. And if the session is still active, it sends a RADIUS disconnect-request message to an appropriate device. This device may not be applying any hot-line rule. Upon receiving the RADIUS disconnect-message, the device terminates the session. If the device is capable of generating accounting messages, it generates a RADIUS accounting-request (stop) message with release indicator (F13) set to 6 (termination due to resource management).

Step 13 Upon receiving the signal to return the user back to normal mode, if the HA is unable to honor the request it responds with a COA NAK packet. Upon receiving a COA NAK, the HAAA may send a RADIUS disconnect-request message to terminate the use's session. The RADIUS disconnect-request message may be sent to the hot-lining device or to another device that is capable of terminating the session. But, if the hot-lining device is able to return the user back to normal state, it sends a COA ACK packet.

Step 14 If the hot-lining device is capable of generating accounting messages it generates a RADIUS accounting-request (stop) message indicating that the hot-lining session has been terminated, and includes the hot-line-accounting indication VSA if received in the COA message. The release indicator (F13) is set to 14 (hot-line status changed).

Step 15 The RADIUS accounting-request (stop) message is followed by a RADIUS accounting-request (start) message indicating the start of the normal packet data session.

Step 16 The user's session is now returned back to normal.

Redundancy Support for Hotlining

In HA Release 5.0 Redundancy framework/infrastructure is modified to be under CCM and Redundancy Framework Inter-device (RF-Interdev).

HA Release 5.1 supports hotlining by downloading a Hotline profile from AAA server using RADIUS attribute 11. HA 5.1 supports hotlining of both new-session and active-session. HA 5.1 also supports hotlining using Change of Authorization messages (COA).

Additionally, HA Release 5.1 supports redundancy for all the above.

The following Hotlining information of binding is synced to standby:

- Hotlining Status—Specifies the current status (Active/Normal) of the binding.
- Hotline Profile(s)—Specifies the hot-lining profile(s) downloaded from AAA using either Radius attribute 11.
- Session-Timeout—Indicates the maximum number of seconds of service to be provided to the user under hotlining.

Additionally, the following information is also synced:

- User-Name—NAI of the user
- Bind address—HoA of the binding.
- Accounting-Session-Id—Accounting Session ID generated by the HA. A new accounting Session ID is generated whenever the user changes the state (from Active to Normal and vice versa).

If the failover occurs and the standby becomes active, it applies the hotline profile to the user. The standby also uses the same Accounting-Session-Id that was synced before failover.

Restrictions and Limitations

The following restrictions and limitations apply to this feature:

- ACL rules that match counters under hotlining are not synced to the standby

Requirements for Hot-Line Capable HA

This section describes the requirements of HA that can be applied to process hot-lining information for MIP flow of a subscriber during Registration/Re-Registration and COA.

1. HA should support both New-Session Hot-Lining and Active-Session Hot-Lining.
2. Hot-Lining should not interfere with the establishment of a packet data session. HA should allow completion of the packet data session and shall allow MIP signaling re-registration. HA shall apply the Hot-Lining rules to DNS traffic and DHCP traffic through relay agent functionality.
   a. During registration of MIP subscriber, if any invalid hot-lining information received by Home-Agent, then HA can reject the RRQ by sending Registration-Reject with "HA-CHAP Failure".
   b. During re-registration of MIP subscriber, HA should retain subscriber MIP Session and as well hot-lining session though the invalid information received in Access-Accept. And, It should reject the RRQ with “HA-CHAP Failure”.
3. HA should include the Hot-line Capability VSA in the RADIUS Access-Request message indicating its ability to support Hot-Lining for MIP subscriber.
4. 4.HA shall treat a RADIUS Access-Accept message as Access-Reject message or shall respond with a COA NAK message with Error-Cause (101) indicating “Administratively Prohibited”(501) when it receives a RADIUS Access-Accept message or COA message that contains:
   a. A RADIUS Filter-Id(11) attribute that it cannot decode.
5. Upon receiving RADIUS Filter-Id(11) attribute(s) in a RADIUS Access-Accept message, HA shall immediately apply the locally provisioned Hot-Line rules that match the one specified by the RADIUS Filter-Id(11) attribute(s).
6. Upon receiving a COA message containing RADIUS Filter-Id(11) attribute(s), HA will locate the Hot-Line rules that match the profile(s) specified by the RADIUS Filter-Id(11) attribute(s). If HA is successful, it should reply to the HAAA with a COA ACK message. HA should remove any previously specified RADIUS Filter-Id(11) attribute(s) and begin applying the rules associated with the newly received RADIUS Filter-Id(11) attribute(s). HA should send accounting messages accounting stop and start messages. If HA is not successful at matching the newly received RADIUS Filter-Id(11) attribute(s) with corresponding rules, it shall send a COA NAK with Error-Cause (101) indicating “Administratively Prohibited”(501). In this case, the Hot-Line state and all existing rules shall remain unchanged.
7. If the HA receives the Session-Timeout (27) attribute it shall terminate the session after the time specified for the session (in seconds) has expired. If HA is capable of RADIUS accounting it shall send a RADIUS Accounting-Request (Stop) message and shall containing the Hot-Lining Accounting Indication VSA if one was received in a RADIUS Access-Accept or COA message.
8. The HA will give priority for the rules that are configured under Profile in the order of HTTP Pass, HTTP Redirection, IPRedirection, IPFilter Rules

9. A Home-Agent that receives the HTTP-Redirection VSA shall monitor the IP flows. When an IP flow matches the "src" and "dst" fields, HA shall apply the rule as specified in the HTTP-Redirection. If the action in the rule is to redirect, HA shall block the traffic and respond to every HTTP request it sees with an HTTP Redirect response (RFC 2616) specifying the URL of the matching HTTP-Redirection Rule VSA.

Limiting the Hot-Lining Duration

Hot-Lined sessions can still utilize expensive network resources, therefore AAA may wish to limit the period over which a session is to be Hot-Lined by sending Session-Timeout atttibute value in either COA or Access-Accept. There are two methods that are available to the operator.

First, a (Hot-Lined or not Hot-Lined) session can be terminated immediately by sending a Disconnect Message. The Disconnect Message is not required to target HA .

Second, the Home RADIUS server should be configured to include the Session-Timeout (27) attribute when it sends the Hot-Lining indication to HA . The Session-Timeout will contain the length of time in seconds varies from 1- (232-1) sec that the user would be allowed to remain in the session. If Session-Timeout expires, the packet data session shall be terminated. This feature will be supported for both profile and rule-based hot-lining.

IP Redirect for Non-Hotlined Users

This feature allows you to configure IP-redirect rules on a per realm basis so that upstream packets can be redirected to the specified IP address. A non-hotlined profile is created and associated with a realm. Under the non-hotlined profile, IP redirect rules are configured.

Once configured, the HA tries to match the packet contents with configured ACL values till Layer-4, and tries to redirect the packets to the configured IP address and port by modifying the destination-ip and destination-port. The destination-port is modified, if the value is configured under profile.

To enable hontlining for non-hotline users, perform the following task:

Command	Purpose
`router(config)# ip mobile home-agent non-hotline profile` *profile-id* `router(non-hotline-rules)# redirect ip access-group {`*100-199 | 2000-2699 | WORD*`} in redirect-ip` *redirect-ip-address* `[redirect-port` *redirect-port*`]`	Enables hotline capability for non-hotline users.

Note This feature is applicable for upstream (MN->Network) traffic only.

Note This functionality is only available for non-hotlined users.

Note NAT functionality must be supported as part of this feature for redirected traffic. This particular functionality is common for both hotlined and non-hotlined user traffic.

Restrictions for Hot-lining

The following list includes restrictions for the Hot-Lining feature:

- In case of upstream traffic, the HA will intercept the traffic and apply HTTP, IP Redirection and IP Filter Rules for the user. In case of downstream traffic, the HA suppports IP Redirection and IP Filter Rules verification. There is no support for HTTP Redirection on the HA for downstream traffic.
- To enable hot-lining on a router, the router should support mobileip and Home Agent functionality. If the router does not, you can enable **router mobile** on the router, and configure **ip mobile home-agent** in global configuration mode.
- Hot-lining capabilities and configuration for any particular user can be overwritten depending on the order in which the Hot-lining CLIs are entered with the latest hot-lining CLI, taking precedence over the previous one. For example, a user "mip1@cisco.com" may have been configured for Profile-based hot-lining. Later, that can be over-written by Rule-based hot-lining configuration.
- Initially a realm configured with hot-lining capabilities that is applicable to all users falls into that realm. Later, that realm can be overwritten to particular user by configuring the user with hot-lining capabilities.
- IOS has restrictions on CLI configuration and deconfiguration. While configuring the CLI the maximum allowed length is 249 characters. For deconfiguring the CLI, the maximum allowed length is 252 characters.

Note The Home Agent MIB is not updated with the Hot-lining information.

Configuring Hot-Lining

To configure Hot-lining, perform the following tasks in global configuration mode:

Command	Purpose

`Router(config)# [no] ip mobile home-agent hotline ?`
`  profile  defines hotline profiles`
`Router(config)# [no] ip mobile home-agent hotline profile word`
`Router(hotline-rules)#`
 	
`Router(hotline-rules)#?`
`  exit  Exit from hotline profile configuration mode`
`  firewall  Defines Firewall filter Rules`
`  no  Negate the hotline rules`
`  redirect  Redirection Rules`
	Enables you to configure and distinguish profile or rule based hot-lining for each user (MN).
	The **profile** keyword acts as sub-configuration mode to configure a set of rules.

`Router(hotline-rules)# [no] Redirect ip access-group {acl-no | word} {in|out} {redirect ip-addr [port]}`	Specifies that IP is the redirected profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.
`Router(hotline-rules)# [no] Redirect http access-group {acl-no | word} {redir-url url}`	Specifies that HTTP is the redirected profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.

Command	Purpose
`Router(hotline-rules)#[no] firewall ip access-group {acl-no | word} {in|out}`	Specifies that IP firewall is the Profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.
`router(config)# ip mobile home-agent non-hotline profile profile-id` `router(non-hotline-rules)# redirect ip access-group {100-199 | 2000-2699 | WORD} in redirect-ip redirect-ip-address [redirect-port redirect-port]`	Enables hotline capability for non-hotline users.

`Router(config)#[no] ip mobile realm {realm | nai} hotline ?`
`capability Hotlining Capability of the mobile hosts`
`redirect Redirect ip address for upstream traffic`
 	
`Router(config)#[no] ip mobile realm { realm | nai} hotline capability ?`
`all Support all Hotline Capabilities`
`httpredir HTTPRedir Rule-based Hot-Lining`
`ipfilter IPFilter Rule-based Hot-Lining`
`ipredir IPRedir Rule-based Hot-Lining`
`profile Profile-based Hot-Lining`
	Configures the hotlining capability of the mobile hose.
	
	Configures either profile, or rule-based hotlining, or all forms of hotlining. The *word* should be specified as **nai | realm**, and in the format of *@cisco.com|username@cisco.com*. Otherwise, this command will give an error message.
	
	At least one form of hot-lining must be selected. There is no default rule to activate rule-based hot-lining for the user. Unconfiguring the command will erase the rule-based hot-lining capability for the user. The values in this configuration are mentioned as flags.
	1 The flag values are explained below.

`Router(config)# ip mobile realm realm hotline capability ipredir`	Configures a profile-based hot-lining for users with IP-redirection rules. Here, the realm can be nai/realm.
`Router(config)#ip mobile realm realm hotline capability httpredir`	Configures a profile-based hot-lining for users with HTTP-redirection rules. Here, the realm can be nai/realm.
`Router(config)# ip mobile realm realm hotline capability rule-based flag`	Configures rule-based hot-lining for users. Here, the realm can be nai/realm.
`router# clear ip mobile traffic`	Clears all ip-mobile related counters for traffic, and clears hotline related counters.

1 The flag values are explained below.

0x00000001 Profile-based Hot-Lining is supported (Using RADIUS Filter-Id attributes)

0x00000002 Rule-based Hot-Lining is supported using Filter Rule

0x00000004 Rule-based Hot-Lining is supported using HTTP Redirection Rule.

0x00000008 Rule-based Hot-Lining is supported using IP Redirection Rule.

For more information related to dynamic ACL configuration, please check the following URL:

http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080430e5b.html

Verifying the Configuration

Perform the following tasks to display various information regarding hotlining on the HA:

Command	Purpose
`Router# show ip mobile hotline[profile profile-id] | summary | users [nai id]`	Displays the hotlined user information for a particular user, or all users eligible for hot-lining.
`Router# show ip mobile hotline users ?` `  nai  MN identified by NAI`	Displays the hot-lined user information for a particular user, or all users eligible for hot-lining.

`Router# show ip mobile hotline profile ?`
`  WORD  Profile-Id`
`  Output modifiers`
	Displays the list of hotline profiles, or particular hotline profile.

`router# show ip mob hot summary`	Displays the list of current statistics of hotline subscribers. This command displays the counters if at least one MIP session should be hot-lined.
`router# show ip mobile traffic [since]`	Incorporates counters for hot-lining sessions (i.e., cumulative counters for number of sessions hotlined, number of active sessions hotlined, number of new session hotlined).

The following is the sample output for hotline user information:

```
HA#show ip mobile hotline users nai mip1@cisco.com
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

HA#show ip mobile hot-lined users
Hotline Binding List:
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

blrmip2@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com
```

The following is sample output for hotline profile information:

```
HA#Show ip mobile hotline profile cisco
Hotline Profile List:
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

HA#show ip mobile hotline profile
Hotline Profile List:
Total 2
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
```

```
    Redirected Url - cisco.com

 Profile: ht-prof1 (Rules 3)
    RuleType IPRedir, Extended ACL Name ht-acl1
    Direction - in
    Redirected IPAddr 16.1.1.102

    RuleType IPRedir, Extended ACL Number 100
    Direction - in
    Redirected IPAddr 1.1.1.1

    RuleType IPFilter, Extended ACL Name cisco
    Direction - out
    HA#
```

The following is sample output for hotline statistics information:

```
HA#sh ip mob hot summary
HomeAgent Hotlining Summary:
    Number of Sessions Hotlined 2
    Number of Profile-Based Hotlined 0
    Number of Rule-Based Hotlined 2
HA#
```

The following is sample output for counters for hot-lining session:

```
HA# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 1351, denied 0, ignored 0, dropped 0, replied 1
    Register requests accepted 1351, No simultaneous bindings 0
    Register requests rcvd initial 149, re-register 1132, de-register 70
    Register requests accepted initial 149, re-register 113, de-register 7
    Register requests replied 1281, de-register 70
    Register requests denied initial 0, 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 0, 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 14, sent 0 total 0 fail 1351
    Binding Update acks received 0 sent 14
    Binding info requests received 0, sent 1 total 2 fail 1
    Binding info reply received 1 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 1
    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 0, 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 SW IDBs: 1 no resource: 0 deleted: 0


Change of Authorization:
  Request rcvd 0, accepted 0
  Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS 0
    Session Cxt Not Found 0, Session Cxt Not Removable 0
    Unsupported Service 0
Dynamic DNS Update (IP Reachability):
Number of DDNS Update Add request sent 0
  Number of DDNS Update Delete request sent 0
Home Agent Hotlining:
    Number of Hotline Sessions 6
    Number of Active-Session Hotlined 0
    Number of New-Session Hotlined 6
    Number of Active-Sessions Reconciled 0
    Number of New-Sessions Reconciled 0
```

CoA for WiMAX Hotlining

Hot-lining can be applied to a new session through an Access-Accept message. Also, an existing session can be hotlined through a change of Authorization (CoA) packet received from the AAA server.

When a CoA (Change of Authorization) packet is received from the AAA server to the HA with in/out ACLs, the In/Out ACL received in the packet is applied to the Subscriber session that could have commands like allow, deny, or re-direct.

In HA5.0, there is no Hot-lining support for Wimax subscribers. Both rule and profile-based hot-lining applied for 3gpp2 subscribers.

The following table illustrates Hot-Lining support for HA Release 5.0 and HA Release 4.0

Technology	Home-Agent Version	Hot-Lining Type Supported	Hot-Lining Style Supported	Redundancy Support
3G (CDMA)	HA4.0	New & Active Session Hot-Lining	Profile and Rule based Hot-Lining	Available
	HA5.0	No	No	No
4G (Wimax)	HA4.0	No	No	No
	HA5.0	No	No	No

In HA Release 5.1, the Home Agent provides support Hot-Lining of Wimax subscribers. The following sub-sections describe detailed call flows for these scenarios.

- This feature supports Wimax new-session and active-session Hot-lining by downloading one or more filter-id [11] attributes from AAA as part of Access-Accept or COA.
- The downloaded filter-id attribute is mapped to one of the profile-ids that is configured locally on the HA. This profile-id consists one or more IP redirection rule and firewall (filter) rules.
- The HA sends Hotline capability in Wimax-capability as sub TLV to the AAA server.

- The HA supports the standard RADIUS attribute Session-Timeout [27] for maintaining the Hotline session, and this approach is downward compatible with HA 4.0 functionality. The user session is restricted to remain hotlined for the duration specified by the hotline-session-timer.
- Whenever the hotline status is modified for subscriber, the HA sends an Accounting Stop and Start for the session. The HA sends and Accounting Stop message with a previously generated/utilized Accounting-Session-Id before the hotline status is modified. The HA generates a new Accounting-Session-Id for sending Accounting Start after modifying the hotline status for the user.
- The Hot-lined MN session is reconciled by downloading the filter- id [11] as “Hot-Line Normal”, either in an Access-Accept during re-registration, or a CoA.
- Since this feature exists on a Single IP architecture, the CP processes the CoA and sends the “InterimUpdate” to the corresponding TP.

Call Flows for Wimax Hot-Lining

The following call flows explain the New-Session and Active-Session Hot-Lining for WiMAX bindings.

New-Session Hot-Lining for WiMAX bindings

1. HA has to send Wimax capability type from the configured value in Access-Request message to AAA server. Required configuration for this is: **ip mobile realm** *realm* **hotline capability** { *ipredir ipfilter httpredir profile all* }
2. During New-Session Hot-lining, HA can receive one or multiple filter-ids [11] with profile-id values that are configured locally on HA. Profile can be configured locally on HA with below CLI: **ip mobile home-agent hotline profile** *profile-id*
3. If HA receives “session-timeout [27]” as part of Access-Accept, then the user will be allowed to remain in the hotline state for the hotline session timer duration mentioned by this attribute. After that, the user will be disconnected.
4. HA will send Accounting Stop and Start whenever hotline status is modified.

Active-Session Hot-Lining for WiMAX bindings

1. During Active-Session Hot-lining, the HA receives one or multiple filter-ids [11] with profile-id values in a CoA message that are configured locally on the HA using the **ip mobile home-agent hotline profile** *profile-id* command.
2. If the HA downloads “session-timeout [27]” as part of the Access-Accept, users can remain in the hotline session only for the hotline session timer duration.
3. The HA sends an Accounting Stop and Start whenever the hotline status is modified.

Re-Conciliation of WiMAX Hotline Session

The term Re-Conciliation represents when a hot-lined user returns back to a normal state. That means the downloaded profiles are no longer applicable for users.

The hot-lined MN session is reconciled by downloading the filter- id [11] value as “Hot-Line Normal”, either in an Access-Accept during re-registration, or in a CoA.

After reconciling the hotline session, the HA sends and Accounting Stop for the previous generated Accounting-Session-Id, and initiates an Accounting-Start by generating a new Accounting-Session-Id.

Note In HA 4.0, in order to reconcile the hotline session, the HA expects the “3GPP2 Hot-Line Normal” string. In Release 5.1, the string value is modified to “Hot-Line Normal”.

Limitations

The following software limitations are noted:

- Configuring HTTP redirection rules under the hot-lining profile configuration is not applicable for Wimax hot-lining support. You can only use the IPFilter and IPRedirect Rule configuration for Wimax hot-lining. As part of this feature support, configuring the HTTP redirection rule is not supported under profile configuration.
- There is no support for Wimax Hotline-Accounting-Indicator as part of this feature.
- For Wimax hot-lining, Rule-based Hot-Lining Rules and Profile-Id, as defined in NWG R1.1 Stage 3, is not supported.
- The Hot-lined MN session can be reconciled by downloading the filter- ids [11] as “Hot-Line Normal”, either in an Access-Accept during re-registration, or in a CoA.

NAT Translations for Hotlining / Non-Hotlining Redirection

The HA has to maintain the mapping between actual destination IP address of the hot-lined or non-hotlined IP redirected user’s data packet and redirected IP address. Whenever a response is received from the redirected server, the HA modifies the response packet src IP address to an actual destination IP address of the request packet.

To perform the mapping between the actual destination IP address/port to the redirect IP address/port, the HA utilizes the NAT Functionality to maintain the NAT Translations during upstream path.

Packet Processing of Upstream Packets

For upstream packets, the HA intercepts the packets after de-capsulation of the tunnel header, and modifies the packet destination IP address to redirected IP address as defined hotline/non-hotline profile information. In case of TCP or UDP Packets, part from modifying the destination IP-address, the HA may modify the destination port address to redirected port address based on availability of redirect port information in hotline/non-hotline profile information. Before finding the adjacency for modified destination IP-address, the HA maintains the NAT translations between the redirected IP-address and actual destination IP-address of the packet. And, the translations also consists of the redirect port and actual destination port information along with **ip**-addresses.

Packet Processing of Downstream Packets

In the downstream path, when a response is received from redirected packets from the redirect server, the HA first finds the adjacency, and based on idb, it hands over the packet to the Home Agent application. The HA looks into NAT translations based on packet information (for example - source IP-address, source port (incase of TCP or UDP packets), ICMP ID (for icmp packets)). The HA fetches the corresponding NAT translation, and modifies the packet source IP-address to the actual destination IP-address. The packets need to be subjected to NAT translations before applying in/out acl, tunnel template and QOS, Hotline/Non-Hotline rules. Later, the HA encapsulates the packet and routes it towards the FA after inspecting the packets with the Home Agent applications.

This functionality can be achieved with NAT support. Here, the HA maintains NAT translations between redirect IP address, the redirect port to destination IP address, and the destination port. The port information is applicable for UDP and TCP packets only.

Create and Maintain the NAT Translations:

- None of the interfaces can be marked as “nat inside” and “nat outside” to maintain the NAT Translations for redirected packets.
- Creating the NAT translations are applicable for upstream hot-lined/non-hot-lined IP redirected packets only.
- TP will only own to create and maintain the NAT translations, CP does not get NAT translations information from individual TPs.

Timeout for NAT Translations

- The HA will internally trigger timer values for NAT translations by invoking NAT APIs during interception of redirected packets for creating translations.
- The timeout values are initialized during configuration of **ip mobile home-agent ipredirect nat-enable** command. The timeout values are not visible on the CP in the **show running-config**, but the TP will display these values.

The following are the Timeouts for different form of packets.

  - For TCP packets, the FIN/RST timeout is 30 Seconds.
  - For TCP packets, the SYN timeout is 30 Seconds.
  - For TCP packets, the timeout is 60 Seconds.
  - For UDP packets, the timeout is 30 Seconds.
  - For ICMP packets, the timeout is 5 Seconds.

- The NAT translation of ICMP packet is timeout after 5 seconds of creation of NAT translations irrespective of response sent by redirected server for translated packet. If the response packet is received from the redirect server within NAT translations expiry (i.e., 5 seconds), the HA re-translates the packet with packet src IP address actual destination IP address.
- For TCP packets, if there is no syn and ack for NAT translated packet on the HA, the HA will timeout for NAT Translations after 20 Seconds.
- For TCP Packets, the HA clears the NAT translations for received FIN or RST packet after 30 seconds.
- For TCP Packets, the HA clears the NAT translation entries after 60 seconds if there is no packet with TCP flags FIN or RST for TCP connection.
- For UDP Packets, the HA clears the NAT translation entries after 30 seconds if there are no packets for corresponding NAT entries.

Redundancy support

There is no redundancy support for updating the NAT translations between the HA redundant peers. During the transition time after switchover between redundant peers, the current active-HA may fail to translate the response packets from redirected server, since it does not have NAT entries for actual requested packets with destination IP-address and redirect IP-address.

Restrictions and Limitations

- Un-configuring this feature CLI command is not permitted when there are active sessions on the Home Agent.
- NAT translations will be cleared on the HA when the timer expiry occurs for each NAT translations, or by removing the translations using the **clear ip nat translations** command. Clearing the MIP sessions and un-configuring the **ip mobile home-agent ipredirect nat-enable** command does not clear the NAT translations.
- CP doesn't show the **ip nat translations** timeout values in the **show running-config**. But, the TP does show these values since data path is supported on TP. For these timer values “write memory” is not required. These values are initiated when is configured with "ip mobile home-agent ipredirect nat-enable" feature.
- HA will take 360bytes of memory to maintain each NAT Translation. From the theoretical calculations,
  - On the 1GB card, each TP can create maximum of 50k translations
  - On the 2GB card, each TP can create maximum of 100k translations.
- Due to deep inspection of packets to create NAT translations and maintain NAT translations, the HA is impacted with a 15-20% of CPU utilization for processing hot-lined redirected packets.