CHAPTER 14

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.

In HA release 3.1, the HA supports profile based hot-lining with IP-Redirection only. In HA release 4.0, the HA support Rule and Profile based hot-lining with all Redirection and Filter Rules, as per the IS 835-D.

Additionally, the Cisco Mobile Wireless Home Agent Release 4.0 supports the following three filters in order to comply with IS.835D standards:

- HTTP Redirection
- IP Redirection
- IP Filter

Additionally, there are two styles used 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.

- In rule-based hot-lining, the home AAA sends actual redirection (HTTP or IP) rules in either an Access-Accept message, or COA radius messages based on the hot-line capability received from the HA during registration in Access-Request. If the HA validates the received rules in the Access-Accept or COA RADIUS messages, the MN packet data session should be hot-lined by applying the rules on user data traffic.
- Firewall hot-lining is applicable for both rule-based and profile-based hot-lining. In rule-based hotlining, the HA receives the IP-Filter-Rule from the home AAA (in either Access-Accept or COA messages) by sending the hot-line capability parameter in an Access-Request.

  In profile-based hot-lining, the IP-Filter-Rule is pre-configured under a particular profile. The HA performs hot-lining after receiving Filter-Id from the home AAA (in either Access-Accept or COA messages) by sending the hot-line capability parameter in and Access-Request.

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.

HA Release 2.0 (and above) supports hot-lining for mobile nodes based on the Nortel X31-20031013-0xx (October 2003). 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.

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).

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 rules 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.

HSRP-HA Redundancy Support for Hot-Lining

Cisco HA Release 3.1 does not support HSRP-HA redundancy for hot-lining feature. Cisco HA Release 4.0 offers redundancy support for rule-based hot-lining; however, it will not support to sync profile-based hot-lining, since HSRP-HA does not have Session Redundancy (SR) functionality.

In the case of rule-based hot-lining, after receiving and validating the COA message content, the active HA will sync part of COA related information to the standby, and even interim syncs occur on the standby whenever rules are updated with COA content by AAA server.

The following information can be synched to standby:

- **User-Name**: the mandatory attribute while syncing rules to standby HA.
- **MN Address**: provided if the MN session (binding) is already established.
- **Hot-Line Accounting Indication**: this field is used when a failover happens to send in accounting messages.
- **Filter-Id**: will specify the hot-lining status for particular user. An active HA that receives more than one filter-id per user should sync to standby-HA. Each filter-id contains either IP or HTTP Redirection rule.
- **Filter-Rules**: contains the IP and HTTP filter rules. It is possible to have more than one filter rule.
- **IP-Redirection-Rules**: contains IP redirection rules. It is possible to have more than one redirection rule.
- **HTTP-Redirection-Rules**: contains IP redirection rules. It is possible to have more than one redirection rule.

- **Accounting-Session-Id**: Provided, if the session is created and user is hot-lined. When a user is hot-lined a new "accounting session id" will be created.
- **Session-Timeout**: Indicates the maximum number of seconds of service to be provided to the user before termination of the session or prompt.

If the failover occurs and the standby become active, it will apply the syncing rules on the user, if session is established and once matching done, the user will be hot-lined. If the session is not established, it will wait till session establishment for particular user.

In redundancy failover, the new active HA will use the same Accounting-Session-Id that was synced before failover.

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. 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; or
   b. A RADIUS Filter-Id(11) attribute and either Filter-Rule VSA(s) or HTTP/IP Redirection-Rule VSA(s); or
   c. Contains Filter-Rule (VSA)s or HTTP/IP Redirection-Rule (VSA)s that it can not 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), HTTP Redirection Rules, IP Redirection Rules, and Filter Rules 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 as described in section 3.1 call flows. 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 HA receives a RADIUS Access Accept message containing HTTP Redirection-Rule VSAs, IP Redirection-Rule VSAs, and/or Filter Rule VSAs that are well-formed (that can be parsed), then the HA shall apply the HTTP Redirection rule(s) if any first, followed by the IP Redirection rule(s) if any ; Filter-Rule VSA(s) if any are processed last. Within each type of rule, the rules are processed in the order that they appear in the packet. In applying the rules (Filter and HTTP/IP Redirection rules), HA should validate the rules against any security policies. If any security policies have been violated, HA shall tear down the user's packet data session.

8. Upon receiving a COA message with well-formed HTTP Redirection Rule, and/or IP Redirection-Rule, and/or Filter-Rule VSAs, HA should validate any locally provisioned filtering that effect local system wide policies. If any of the rules violate local policies, or HA is not able to accept the COA message, it shall send a COA NAK message with Error-Cause (101) indicating "Administratively Prohibited" (50). In this case, the Hot-Line state and all existing rules shall remain unchanged. Otherwise, when no rules violate local security policy, HA shall do the following:

   a. If HA is currently applying rules associated with a previously received RADIUS Filter-Id(11) attribute(s), it stops applying the rules associated with the previously received RADIUS Filter-Id(11) attributes and begins applying the newly received HTTP Redirection Rules, and/or IP Redirection Rules, and/or Filter Rules. HA shall respond to the HAAA with a COA ACK and begin sending accounting messages as described in section 3.1 call flows.

   b. If HA is currently applying rules associated with previously received HTTP Redirection Rules and/or IP Redirection Rules and/or Filter Rules, it shall overwrite any old rules of the same kind (HTTP with HTTP, IP with IP, Filter with Filter) with the new rules. If no old rules of the same kind exist, the new rules of that kind shall be applied. HA shall respond to the HAAA with a COA ACK and begin sending accounting messages as described in section 3.1 call flows.

9. If 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.

10. 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 VSA. 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.

11. The following explanation will take care about "Loop in the Hot-Lining HTTP Redirection Rule"

   a. “Loop in the Hot-Lining HTTP Redirection Rule” means, initially HA receives a HTTP Redirection Rule "redirect www.cisco.com from 10.1.1.0/8 to 192.168.1.0/8". HA will redirect the HTTP packet to www.cisco.com by initiating Redirect 302 message to MN subscriber, when above rule conditions are matching. MN will send fresh HTTP Request Get message with received redirected URL. But, the Redirected-url is mapped to one of the address of subnet 192.168.1.0/8 i.e., 192.168.1.100. Then, HA will again initiate HTTP-302 Redirect message to MN for received HTTP-302 message. And, this mechanism continues between MN and HA as long as TCP session established between MN and HTTP Server through HA. To avoid this looping mechanism, the following rule needs to be downloaded from AAA along with HTTP Redirection Rule.

   “pass from 10.1.1.0/8 to 192.168.1.100/0”

   “redirect www.cisco.com from 10.1.1.0/8 to 192.168.1.0/8”

   And the “HTTP-Pass Rule” should always preceded by “HTTP-Redirection Rule” to avoid looping mechanism.

12. A Home-Agent that receives the IP-Redirection rule VSA shall monitor the IP flows. When an IP flow matches the rule, HA shall redirect the flow to the address specified in the matching rule.
13. A Home-Agent that receives the IP-Filter rule VSA shall monitor the IP flows. When an IP flow matches the rule, HA depending on the specified action shall either block or allow the flow to proceed.
14. A Home-Agent that receives an HTTP Redirection Rule, an IP-Filter-Rule or an IP-Redirection-Rule that contains the keyword "flush" shall flush all previously received attributes of the same kind for that session.
15. If HA receives an Access-Accept or a COA with the Hot-Line Accounting attribute but no RADIUS FIlter-Id(11) attribute(s)/HTTP Redirection Rule VSA/IP Redirection Rule VSA/Filter Rule VSA then this Hot-Line Accounting-Indication shall not affect the Hot-Line state of the user. If HA is capable of generating RADIUS accounting messages then it shall include the newly received Hot-Line Accounting Indicator in all subsequent accounting messages.

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.

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.
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)#[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.

Command	Purpose
`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
```