



CHAPTER 13

Monitoring Upstream User Traffic

This chapter discusses how to monitor upstream 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, page 13-1](#)
 - [Active Session Hot-Lining, page 13-1](#)
 - [New Session Hot-Lining, page 13-2](#)
 - [Restrictions for Hot-lining, page 13-2](#)
 - [Configuring Hot-Lining, page 13-3](#)

Hot-lining

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 Home AAA server (HAAA) is the User-Name attribute to identify the particular user on the Home Agent. Optionally, the IP address can also be sent in the CoA message to identify the particular binding for a particular user.

Active Session Hot-Lining

For active session hot-lining, the user starts a packet data session. In the middle of the session it is hot-lined and, after the account is reconciled, hot-lining on the session is removed. Hot-lining is done with a RADIUS Change of Authorization (CoA) message. The following procedure lists the events for active session Hot-lining:

-
- Step 1** Action for normal hot line profile is locally configured on the HA.
 - Step 2** Action for active hot line profile is locally configured on the HA.
 - Step 3** User joeusr@carrier.com is created at the Home AAA and assigned a normal hot line profile.
 - Step 4** User joeusr@carrier.com registers with the HA.

- Step 5** The HA sends an Access Request to the HAAA for the user.
 - Step 6** The HAAA responds with an Access Accept that contains a Filter-ID attribute set to normal.
 - Step 7** The HA applies normal hot line action (no redirection) for the user.
 - Step 8** The HA completes MIP registration by sending an RRP.
 - Step 9** Some event occurs at this point to cause the user to be hot lined. The user hot line profile at the HAAA is modified to active.
 - Step 10** The HAAA sends a Change of Authorization command with Filter-ID attribute set to active.
 - Step 11** The RADIUS client at the HA ACKs the Change of Authorization command.
 - Step 12** The HA applies active hot line action (redirection) for the user.
 - Step 13** At this point, the user has taken action to reconcile the event that resulted in hot lining of the account. The hot line profile at the HAAA is modified to normal.
 - Step 14** The HAAA sends a Change of Authorization command with Filter-ID attribute set to normal.
 - Step 15** The RADIUS client at the HA ACKs the Change of Authorization command.
 - Step 16** The HA applies normal hot line action (no redirection) for the user.
-

New Session Hot-Lining

For new Session hot-lining, the user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session. The following procedure lists the events for new session hot-lining:

- Step 1** Action for normal hot line profile is locally configured on the HA.
 - Step 2** Action for active hot line profile is locally configured on the HA.
 - Step 3** User joeusr@carrier.com is created at the HAAA and assigned an active hot line profile.
 - Step 4** User joeusr@carrier.com registers with the HA.
 - Step 5** The RADIUS client sends an Access Request for the user.
 - Step 6** The Access Accept contains the Filter-ID attribute set to active.
 - Step 7** The HA applies active hot line action (redirection) for the user.
-

Restrictions for Hot-lining

The following list identifies restrictions for the hot-lining feature:

- The hot-lining feature supports only upstream IP packet level re-direction and downstream packets are not hot-lined. Firewall hot-lining is not supported.
- The Home Agent does not support Correlation ID and NAS-Identifier attributes in the CoA request received from AAA.
- Hot lining is not supported with HA redundancy.
- On the Home Agent, the hot-lining policy is applied only when the policy is downloaded during HA CHAP.

- The Home Agent will not reject the RRQ if reverse-tunnel is not requested by the user and hot lining policy is downloaded for the user.
- The Home Agent will not notify packet data users the reason for their hot-lined status prior to denial of data service.
- 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)# ip mobile realm realm hotline redirect <i>redirect-server-ipaddress</i>	Enables inbound user sessions to be disconnected when specific session attributes are presented.
ip mobile cdma-ipsec fa-address ip address security-level 1 2	<i>ip address</i>

