Configuring Hotlining for a Home Agent

SYSTEM ADMINISTRATOR GUIDE

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Overview

This document provides an overview of hotlining for a home agent (HA) using the SmartEdge® OS and describes the tasks used to configure this feature. This document also provides configuration examples of hotlining for an HA.

Note: This document describes hotlining for an HA only. For information on using the SmartEdge OS to for hotlining for an FA, see *Configuring Hotlining for a Foreign Agent* .

Hotlining allows WiMAX operators to efficiently redirect subscribers to a portal controlled by a service provider for service registration, updates, service advertisements, and address issues that require immediate attention, such as virus attacks and missed payments. When hotlining is complete, the subscriber is released from the hotlined state (released from the portal) and to the original destination.

For example, if a subscriber has a mobile device that is locked to a subscription with a service provider, that subscriber can be hotlined to a subscription server when the device is turned on. No other traffic is allowed. The subscription server provides subscription options that the subscriber can choose from. When the subscriber completes the subscription process, the subscriber is removed from the hotlined state.

Note: Hotlining is WiMAX feature that supports only WiMAX subscribers.

There will be accounting discrepancies of a few bytes per packet when the HA receives packets containing IP and GRE field values.

If the shared-key is configured using the **`subscriber default mobile-ip shared-key`** command, the SmartEdge OS treats the subscriber as a 3GPP2 user.

The HTTP get request packets that hit the home agent do not get counted as part of hotline counters if the session was hotlined at the time the get packets were sent. Once the session is redirected, the redirected packets are counted as part of hotline service counters.

When a hotlining session is activated, the HA receives the WiMAX Forum RADIUS VSA, Hotline-Profile-ID (the hotlining profile identifier attribute), and Hotline-Indicator attribute (an attribute that enables hotlining) from the AAA server in a RADIUS Access-accept or change of authorization message (CoA). These attributes enable hotlining. The hotlining profile identifier selects a preconfigured profile during the session. The RADIUS server or CoA sends the WiMax Forum RADIUS VSA Hotline-Indicator attribute in the Access-Accept or COA-Request message, which is reported in the session and hotlining accounting records. For information on hotlining RADIUS attributes (Hotline-Profile-ID and Hotline-Indicator), see *WiMax Forum RADIUS VSAs* and *WiMax Forum RADIUS VSAs in the CoA* in *RADIUS Attributes*.

The following are key accounting attributes in SmartEdge router RADIUS accounting records that distinguish hotline accounting records from session accounting records and start records from stop records:

(A) SESSION-ACCT-START

Acct-Status-Type = Start

(no Hotline-Indicator)

Acct-Session-ID = <generated-id-2

Acct-Multi-Session-ID = <multi-session-id-1>

(no counters)

(B) SESSION-ACCT-STOP (session stop, hotlining begin)

Acct-Status-Type = Stop

Acct-Session-ID = <generated-id-2>

(no Hotline-Indicator)

(no Acct-Terminate-Cause)

Acct-Multi-Session-ID = <multi-session-id-1>

Counters

(C) SESSION-ACCT-STOP (regular session down)

Acct-Status-Type = Stop

(no Hotline-Indicator)

Acct-Terminate-Cause = <some cause code)

Acct-Session-ID = <generated-id-2>

Acct-Multi-Session-ID = <multi-session-id-1>

Counters

(D) HOTLINE-ACCT-START

Acct-Status-Type = Start

Hotline-Indicator = <hl-ind-1> (from AAA server)

Acct-Session-ID = <generated-id-1>

Acct-Multi-Session-ID = <multi-session-id-1>

(no counters)

(E) HOTLINE-ACCT-STOP (hotline stop, begin regular session)

Acct-Status-Type = Stop

Hotline-Indicator = <hl-ind-1>

Acct-Session-ID = <generated-id-1>

(no Acct-Terminate-Cause)

(no counters)

(F) HOTLINE-ACCT-STOP (session down from hotlining)

(no counters)

Acct-Status-Type = Stop

Hotline-Indicator = <hl-ind-1>

Acct-Session-ID = <generated-id-1>

Acct-Terminate-Cause = <some cause code>

For information about the Acct-Terminate-Cause attribute, see *RADIUS Attributes*.

2 Configuration Tasks

Note: Hotlining is a WiMAX feature that supports only WiMax subscribers. Hotlining does not support IP and GRE header field values in packets

To configure hotlining, perform the tasks described in the following sections:

2.1 Configure the Local HTTP Server on the Active Controller Card

To configure the HTTP server on the active controller card, perform the tasks described in Table 1.

Note: In this section, the command syntax in the task tables displays only the root command.

Table 1 Configure the HTTP Server on the Controller Card

#	Task	Root Command	Notes
1.	Enable the HTTP server on the controller card and access HTTP redirect server configuration mode.	*http-redirect server*	Enter this command in global configuration mode.
2.	Optional. Select the port on which the HTTP server listens.	*port (http)*	Enter this command in HTTP redirect server configuration mode.

2.2 Configure a RADIUS Server Profile

To configure a RADIUS server profile, perform the task described in Table 2.

Table 2 Configure and Attach an HTTP Redirect Profile to Subscribers

#	Task	Root Command	Notes
1.	Create or select RADIUS-guided service profile and accesses service profile configuration mode.	*radius service prof ile*	Enter this command in context configuration mode. For more information about RADIUS configuration, see *Configuring RADIUS*.

2.3 Configure a Policy ACL That Classifies HTTP Packets

To configure a policy access control list (ACL) that classifies HTTP packets for the forward policy that redirects HTTP packets, perform the tasks described in Table 3.

Table 3 Configure a Policy ACL That Classifies HTTP Packets

#	Task	Root Command	Notes
1.	Create or select the policy ACL and enter access control list configuration mode.	*policy access-list*	Enter this command in context configuration mode. This profile is the one selected by the value of the WiMAX attribute Hotline-Profile-Id. For more information about ACLs, see *Configuring ACLs*.
2.	Assign HTTP packets that are destined to the web server hosting the URL to a separate class.	*permit*	Enter this command in access control list configuration mode. Use the following construct: **`permit tcp any host`*`ip-addr`*`eq www class`** *`class-name`* Where the *`ip-addr`* argument is the IP address of the web server hosting the URL that you configured in step 2 in Table 2.
3.	Assign all other HTTP packets to a different class.	*permit*	Enter this command in access control list configuration mode. Use the following construct: **`permit tcp any any eq www class`** *`class-name`* Where the *`class-name`* argument is distinct from the one that you configured in step 2.

2.4 Configure a Forward Policy to Redirect HTTP Packets

To configure a forward policy to redirect HTTP packets, perform the tasks described in Table 4.

Table 4 *Configure and Attach a Forward Policy to Redirect HTTP Packets*

#	Task	Root Command	Notes
1.	Create or select the forward policy and access forward policy configuration mode.	*forward policy*	Enter this command in global configuration mode. For more information about forward policies, see *Configuring Forward Policies*.
2.	Apply the policy ACL that you configured in Table 3 to the forward policy and access policy ACL configuration mode.	*access-group*	Enter this command in forward policy configuration mode.
3.	Specify all HTTP packets and access policy ACL class configuration mode.	*class*	Enter this command in policy ACL configuration mode. Use the `class-name` argument that you specified in step 3 in Table 3.
4.	Redirect HTTP packets to the HTTP server on the controller card.	*redirect destination local*	Enter this command in policy ACL class configuration mode.

2.5 Configure Accounting Server

To configure an accounting server, perform the tasks described in Table 5.

Table 5 *Configure and Attach a Forward Policy to Redirect HTTP Packets*

#	Task	Root Command	Notes
1.	Create or select the forward policy and access forward policy configuration mode.	*radius accounting server*	Enter this command in context configuration mode. For more information about RADIUS configuration, see *Configuring RADIUS*.

3 Configuration Examples

This section provides examples of configuring an HA and RADIUS entry.

3.1 Hotlining for an HA Configuration Example

The following example shows a HTTP redirect configuration:

```
!First enable the HTTP redirect server on the controller card.

[local]Redback(config)#http-redirect server
[local]Redback(config-hr-server)#port 80
[local]Redback(config-hr-server)#exit

!Configure the RADIUS profile:

[local]Redback(config)#context local
[local]Redback(config-ctx)#radius service profile wimax-h1-prof-3
[local]Redback(config-service-profile)#accounting in circuit
[local]Redback(config-service-profile)#accounting out circuit
[local]Redback(config-service-profile)#attribute forward-policy fwd-pol-1
[local]Redback(config-service-profile)#attribute http-redirect-url
"http://my-redir-url.funky.com"
[local]Redback(config-hr-profile)#exit

!Configure the ACL policy.

[local]Redback(config-ctx)#policy access-list http-packets-1

!class PORTAL allows HTTP from “any” to the redirected web server at
10.1.1.1

[local]Redback(config-access-list)#permit tcp any host 10.1.1.1 eq www
class PORTAL

!Specify that packets that are not part of the PORTAL class get
redirected to the local HTTP.

[local]Redback(config-access-list)#permit tcp any any eq
www class REDIRECT
[local]Redback(config-access-list)#permit tcp any any eq
www CATCH-ALL
[local]Redback(config-ctx)#exit

!Create the forward policy.
```

```
[local]Redback(config)#forward policy www-redirect-1

!Apply the ACL policy that classifies HTTP packets.

[local]Redback(config-policy-frwd)#access-group http-packets-1
local

!Redirect all REDIRECT class packets to the local HTTP server on the
SmartEdge
 router.

[local]Redback(config-policy-group)#class REDIRECT
[local]Redback(config-policy-group-class)#redirect
destination local
[local]Redback(config-policy-group-class)#exit

!Class PORTAL packets destined for the redirected web server typically
get routed to the portal.

[local]Redback(config-policy-group)#class PORTAL
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class CATCH-ALL
[local]Redback(config-policy-group-class)#drop
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-frwd)#exit

!Configure a RADIUS accounting server IP address of 10.3.3.3 with the
key, secret, using port 4445 for accounting.

[local]Redback(config-ctx)#radius accounting server 10.3.3.3 key
secret port 4445
```

3.2 RADIUS Entry Example

The following RADIUS entry applies the forward policy at hotline activation time by referring to it from the RADIUS service profile configured on the SmartEdge router:

```
WiMAX-Hotline-Profile-ID= "wimax-hl-prof-3",
WiMAX-Hotline-Indicator="ABCDEF",
WiMAX-Capability = "\002\003\001"
```