ERICSSON

Configuring Hotlining for a Foreign Agent

SYSTEM ADMINISTRATOR GUIDE

39/1543-CRA 119 1170/1 Uen D

Contents

1 Overview

This document provides an overview of the SmartEdge® OS hotlining features and describes the tasks used to configure these features. This document also provides configuration examples of hotlining features.

In a WiMAX network, the SmartEdge router functions as an Access Serving Network-Gateway (ASN-GW) Enforcement Point (EP) that activates hotlining rules passed by the ASN-GW Decision Point (DP). In this configuration, the SmartEdge router supports hotlining services for mobile foreign agent (FA) users, providing WiMAX operators with a self-subscription service that handles user-related issues which would otherwise result in service denial.

When configured as an ASN-GW EP, the SmartEdge router filters and redirects traffic for users based on the set of rules obtained from the ASN-GW DP. Hotlining is activated when the SmartEdge router receives the hotline indicator vendor-specific attribute (VSA) and HTTP redirection rules from the ASN-GW DP. The network access server (NAS) filter rules are also sent to the SmartEdge router, if required.

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.

In a WiMAX network where the SmartEdge router functions as an ASN-GW EP, a subscriber is hotlined as follows:

1. A new mobile user without subscription sends an IP registration request to the network.

2. The home authentication, authorization, and accounting (H-AAA) device grants the user limited access to the network and sends a RADIUS Access-Accept message to the ASN-GW DP with hotlining status of the user. The RADIUS Access-Accept message contains the HTTP redirect rules and NAS filter rules that determine what kind of traffic is permitted in the WiMAX network.

3. The ASN-GW DP sends information about the user (including hotlining instructions) to the SmartEdge ASN-GW EP through an R7 interface.

4. The user is hotlined, the SmartEdge ASN-GW EP filters and redirects uplink traffic from the user to the Captive Portal based on the set of redirect rules obtained from the ASN-GW DP, and a new user account is created with information for the user.

5. The subscriber management server informs the Open Mobile Alliance (OMA) Device Management (DM) application that a new mobile station (MS) needs to be managed. If the OMA DM application bootstraps the MS

to update the software or provision data on the MS, then the OMA URL is sent to the MS. The MS uses the OMA URL to perform provisioning.

From this point on, the HTTP traffic is redirected to the OMA-DM instead of the Web Portal. Because the Web Portal and the OMA-DM are in different domains, the packet identification for traffic to OMA-DM is different from the traffic to Web Portal.

When the hotlining subscription process is finished, the SmartEdge ASN-GW EP removes the HTTP and IP redirect and filter rules and normal data sessions resume.

1.1 Hotlining Rules and Restrictions

Keep the following rules and restrictions in mind when configuring a SmartEdge router as an ASN-GW EP:

- You must perform one of the following configurations on the SmartEdge router for hotlining to function:
  - Enable RADIUS authentication configuration in the FA context.
  - Enable RADIUS authentication configuration in the local context, and reference that configuration in the FA context.
- Both new-session and midsession IP hotlining are supported.
- Only one redirect URL is supported.
- Up to 20 NAS filter rules are supported for each subscriber. Note that the total length of the attributes in the RADIUS message cannot exceed 4000 bytes.
- An individual VSA for a rule cannot exceed 253 bytes. Note that the VSA includes a 7-byte TLV overhead, so the actual size of the rule is 246 bytes.
- Each HTTP redirection rule is typically contained in a single VSA; however, NAS filter rules can span multiple attribute boundaries. Note, however, that the SmartEdge router verifies only conformance to RADIUS message and VSA size limits. The ASN-GW DP imposes limits on the rule sizes and ensures that enough space exists to send all required VSAs in a single RADIUS message.
- If an application of new rules fails, note that the old rules do not replace new rules, but the subscriber is retained.
- If the ASN-GW DP sends the SmartEdge ASN-GW EP an HTTP redirection rule VSA that is redirected to a URL, the SmartEdge ASN-GW EP verifies that at least one HTTP redirection rule VSA exists that contains the IP address to which the HTTP traffic is passed.

- The hotlined state of a user is maintained across subscriber moves that may result in slot or port changes.
- The SmartEdge ASN-GW EP logs hotlining rule failures for each subscriber. Counters capture the number of rules failures and rule successes for each subscriber.
- If a subscriber is hotlined before a configuration change that disables per-MS services on the R7 interface, the subscriber remains hotlined until the session times out.
- Because accounting is not enabled on the R7 interface, the following mismatches can occur:
  - If a hotlining session is administratively cleared on the SmartEdge ASN-GW EP, the R7 interface is not informed that the session is clear.
  - If the idle timeout is configured for a hotlining session on the SmartEdge ASN-GW EP, the session is cleared when the timeout interval expires.
  - If errors occur while synchronizing the session to the standby, the session is cleared on the SmartEdge ASN-GW EP but remains active on the R7 interface.

In an ASN-GW EP configuration, the SmartEdge router supports the following hotlining features:

- Hotlining activation and deactivation.
- Notification to the ASN-GW DP when hotlining provisioning for a subscriber succeeds or fails. If enabled in the Accounting-Mode VSA, the SmartEdge ASN-GW EP notifies the ASN-GW DP upon succession or failure of hotlining provisioning for a subscriber. An accounting start message from the SmartEdge indicates provisioning success, while an accounting stop message indicates a provisioning or parsing failure. The reason a hotlining session is rejected is included in the accounting stop message. Accounting start and stop messages are sent after a provisioning's outcome is known. If an account message is lost during a restart, then that start message is not resent. Accounting start and stop messages contain the required accounting attributes from the VSA table. Any additional attributes are ignored.

1.2 NAS Filter and HTTP Redirection Rules

The R7 interface transfers the following hotlining rules from the ASN-GW DP to the ASN-GW EP:

- NAS filter rules that determine the types of traffic is permitted or denied by the WiMAX network.
- HTTP redirection rules that determine the URL to which packets are redirected. Two types of HTTP redirection rules exist: pass rules and

redirect rules. Pass rules forward packets to a particular IP address, and redirect rules redirect the packets to a specified URL.

The SmartEdge OS can receive and apply any combination of the following hotlining rules to the FA:

- Only NAS filter rules, if received from the ASN GW DP.
- Only HTTP redirection rules. In this case, non-HTTP traffic can still pass through the ASN GW EP, if required by the operator.
- HTTP redirection rules and NAS filter rules that are received from the ASN-GW DP.

Note: Both NAS filter and HTTP redirection rules are applied in the order received by the ASN GW DP. However, NAS filter rules are always applied before HTTP redirection rules.

Note: If HTTP redirection rules are present, at least one pass rule and one redirect rule must exist. A pass rule must be present before a redirect rule can be applied.

For a new hotlining session, hotlining attributes are sent in an Access-Accept message. For midsession hotlining, the hotlining rules are sent in a CoA message.

Note: The SmartEdge OS supports only one HTTP redirect URL.

NAS filter rules determine whether the system permits or denies access to incoming packets based on the type of information in the IP packet headers. NAS filter rules are sent in every CoA message in the following circumstances:

- When new NAS rules need to be applied.
- When one or more NAS rules need to be removed.
- When one or more NAS rules need to be replaced.
- When the existing NAS rules need to be retained.

NAS filter rules are evaluated in the order received. Each packet is evaluated once, and the first matched rule terminates the evaluation process. If no rules match, the packet is dropped. Packets are filtered based on the information in Table 1.

Table 1 Supported NAS Filter Rules

Filter	Rules
Action	Determines whether the packet is permitted or denied on the destination router. Can be one of the following: • permit —Allow packets that match the rule. • deny—Drop packets that do not match the rule.

Table 1 Supported NAS Filter Rules

Filter	Rules
Direction	Defines whether the packet is arriving from or leaving the terminal. Can be one of the following: • in—Packets arriving from the terminal. • out—Packets leaving the terminal.
Proto	Specifies an IP protocol. Packets that have a matching IP keyword are permitted.

Table 1 Supported NAS Filter Rules

Filter	Rules
src/dst	Specifies the source-and-destination address or mask and the port for a packet. Can be expressed in any of the following formats: • ipno —IPv4 number in dotted-quad or canonical form. Only those packets with an IP number that matches this rule exactly are permitted. Note that IPv6 is not supported. • ipno bits—IP number specified in the format ***address*/*mask***. The bit width must be valid for the IP version, and the IP number cannot have bits set beyond the mask. For a match to occur, the same IP version must be present in the packet IP address. • any—Source-and-destination IP address is 0.0.0.0/0. Packets that have any IP address are considered a match are permitted. • assigned—Address or set of addresses assigned to the terminal. Packets that have an IP address that matches the assigned address are permitted. • ports—Optional source and destination ports. For the TCP, UDP, and SCTP protocols, the optional ports are specified in the format ***ports*/*port*-*port***[,***port***[...]] • src / dst “assigned”——Address or set of addresses assigned to the terminal. Packets that have a matching address are permitted. • port range—Range of ports. Packets whose destination port matches one of the ports in this range are permitted.
IP Options	Determines which packets are permitted or denied. The following TCP flags are supported: - established—Packets that have the RST or ACK bits set are permitted. Note that this flag applies to TCP packets only. - setup—Packets that have the SYN bit set and no ACK bit are permitted. Note that this flag applies to TCP packets only. - Icmptypes types—Packets that have one or more of the following ICMP types are permitted. Note that each type is represented by a number: • 0—echo reply • 3—destination unreachable • 4—source quench • 5—redirect • 8—echo request • 9—router advertisement • 10—router solicitation • 11—excessive time-to-live • 12—bad IP header • 13—time stamp request • 14—time stamp reply • 15—information request • 16—information reply • 17—address mask request • 18—address mask reply Note that the SmartEdge router supports those rules received with one ICMP type only or several ICMP types that are separated by commas. If a rule has multiple ICMP types, each type must be separated by a comma. The list of multiple ICMP types is converted into individual rules for each ICMP type. Note that the Icmptypes types flag applies to ICMP packets only.

The SmartEdge ASN-GW EP does not allow subscriber traffic to pass if the traffic does not conform to the hotlining rules until all rules have been applied on the line cards. Control traffic, such as MIP control traffic, is processed when received. The ASN-GW DP sends the NAS filter rules to ASN-GW EP to permit RRQ traffic.

The SmartEdge FA cannot apply a new set of hotlining HTTP redirection rules to a subscriber that has already been hotlined. To apply a new set of hotlining rules, hotlining is first deactivated on the subscriber and then reactivated with the new set of rules.

Note: The performance of the SmartEdge router may be impacted if the number of rules received is large because of the overhead required to process the rules for each subscriber.

Table 2 lists the RADIUS attributes that are included in the following messages:

- Access request messages—sent from the ASN-GW EP to the ASN-GW DP for new sessions.
- Access-accept—Sent from the ASN-GW DP to the ASN-GW EP for new sessions.
- CoA—Sent from the ASN-GW DP to the ASN-GW EP for midsession hotlining.
- Accounting start—Sent from the ASN-GW EP to the ASN-GW DP if accounting is enabled in the Accounting-Mode VSA.
- Accounting stop—Sent from the ASN-GW EP to the ASN-GW DP if accounting is enabled in the Accounting-Mode VSA.

Table 2 RADIUS Attribute Support

Attribute	access request	access-accept	CoA message	accounting Start	accounting Stop
User-Name	Yes	Yes	Yes	Yes	Yes
Calling-station-ID	Yes	Yes	Yes	Yes	Yes
Message Authenticator	Yes	Yes	No	No	No
NAS-IP-Address	Yes	No	No	Yes	Yes
EP-Request-Type	Yes	No	No	No	No
CoA-IPv4	Yes	No	No	No	No
AAA-Session-ID	No	Yes	Yes	Yes	Yes
Accounting-Mode	No	Yes	No	No	No
Hotline-Indication	No	Yes	Yes	No	No
HTTP-redirection-rule	No	Yes	Yes	No	No
NAS-filter-rule	No	Yes	Yes	No	No
FA-hHA-Key	No	Yes	No	No	No
FA-hHA-SPI	No	Yes	No	No	No

Table 2 RADIUS Attribute Support

Attribute	access request	access-accept	CoA message	accounting Start	accounting Stop
FA-hHA-Lifetime	No	Yes	No	No	No
FA-vHA-Key	No	Yes	No	No	No
FA-vHA-SPI	No	Yes	No	No	No
FA-vHA-Lifetime	No	Yes	No	No	No
hHA-IP-MIP4	No	Yes	No	No	No
vHA-IP-MIP4	No	Yes	No	No	No
Acct-Status-Type	No	No	No	Yes	Yes
Acct-Term-Cause	No	No	No	Yes	Yes
Acct-Multi-Session-ID	No	No	No	Yes	Yes
Session_Error_Message	No	No	No	No	Yes
Error-Cause	No	No	Yes (in CoA NAK messages only)	No	No

Note: If multiple unique URLs are received in HTTP redirection rules, a provisioning error is reported to the R7 interface because only one URL is supported per subscriber.

Note: Any Hotline-Profile-ID attribute that is received in an Access_Accept or CoA message is rejected.

Note: Any Hotline-Session-Timer attribute that is received in an Access_Accept or CoA message is ignored.

Note: When an access request is rejected, an Access Reject message is sent with the User-Name and Message Authenticator attributes.

Note: The Acct-Multi-Session-ID attribute is sent only when the AAA-Session-ID attribute is received for hotlining and NAS filter rules provisioning.

1.3 Hotlining Deactivation

Hotlining is deactivated when the ASN-GW DP sends the SmartEdge ASN-GW EP a RADIUS CoA request that contains a hotline-indicator VSA with a null value or that does not have a hotline-indicator VSA. HTTP Redirection rules with a flush action are included. If new NAS filter rules are included in the COA-Request, the ASN-GW EP replaces the pre-existing NAS Filter rules with the new NAS filter rules. If the COA-Request contains NAS Filter rules with a null value, the existing NAS filter rules are removed for the affected subscriber.

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

2.1 Configuring Hotlining Services for an FA

To configure hotlining services for an FA, perform the tasks described in Table 3.

Table 3 Configuring Hotlining Services for an FA

#	Task	Root Command	Notes
1.	Configure the local HTTP server on the active controller Card, as described in “Configure the Local HTTP Server on the Active Controller Card” earlier in this document.		
2.	Configure the RADIUS server to send the hotlining rules:		
	Configure context-specific RADIUS authentication.	**`aaa authentication subscriber radius`**.	For more information about configuring RADIUS authentication, see *Configure Subscriber Authentication*.
	Identify the RADIUS server from which hotlining rules are received.	**`radius server`** {***`ip-addr`*** | ***`hostname`***} **`encrypted-key`** ***`key`***	Use the ***`ip-addr`*** or ***`hostname`*** argument to specify the RADIUS server from which the SmartEdge router receives hotlining rules. Replace the key argument with the authentication key that must be shared with the RADIUS server. For more information about configuring a RADIUS server, see *Configuring RADIUS* .
	Configure a CoA server from which CoA messages are accepted.	**`radius coa server`** {***`ip-addr`*** | ***`hostname`***} **`key`** ***`key`***	AAA accepts messages from this server only. Use the ***`ip-addr`*** or ***`hostname`*** argument to specify the RADIUS server from which the SmartEdge router receives hotlining rules. Replace the ***`key`*** argument with the authentication key that must be shared with the CoA server.
3.	Configure the accounting server.		

Table 3 Configuring Hotlining Services for an FA

#	Task	Root Command	Notes
	Identify a RADIUS accounting server to be used if the accounting mode is enabled for the subscriber.	**radius accounting server** {***ip-addr*** | ***hostname***} **key** ***key***	Use the ***ip-addr*** or ***hostname*** argument to specify the RADIUS accounting server from which the SmartEdge router receives hotlining rules. For more information about configuring a RADIUS accounting server, see *Configuring RADIUS* .
	Enable the accounting server to receive accounting packets from AAA.	**aaa accounting subscriber radius attribute-guided**	Enter this command in context configuration mode. This command ensures that the RADIUS accounting server is ready to send and receive accounting packets. Note that accounting packets are sent to a subscriber only when the Accounting-Mode VSA is present in the authentication response that is received from the subscriber. For more information about configuring subscriber accounting on the SmartEdge router, see *Configure Subscriber Accounting* .
4	Configure a RADIUS-guided forward policy with PASS, REDIRECT, and DROP classes. For general information about configuring forward policies, see *Configure a Forward Policy*.		
	Select a RADIUS-guided forward policy and access forward policy configuration mode.	**forward policy name radius-guided**	Replace the ***name*** argument with the name of the forward policy you want to access. Note that no default configuration must exist for the forward policy because the configuration translates to a pass action for default class traffic.
	Access policy group configuration mode.	**access-group**	
	Create a class called “redirect” and access policy group class configuration mode.	**class redirect**	
	Redirect incoming packets associated with the specified class to the local server.	**redirect destination local**	

Table 3 Configuring Hotlining Services for an FA

#	Task	Root Command	Notes
	Exit policy group class configuration mode.	`exit`	
	Create a class called “pass” and access policy group class configuration mode.	`class pass`	
	Create a class called “drop” and access policy group class configuration mode.	`class drop`	
	Exit policy group class configuration mode.	`exit`	
	Configure the router to drop incoming packets for this forward policy	`drop`	
5.	Configure the RSE profile with the forward policy. For more information on configuring a RADIUS service profile that references RADIUS-guided policies, see *Configure a RADIUS-Guided Service Profile* in *Configuring RADIUS* .		
	Select an existing RSE profile or create a new RSE profile and access service profile configuration mode.	`radius service profile`	Enter this command in context configuration mode. Map this profile to the FA subscriber rules.
	Specify a service condition for the redirect service profile and its default condition.	`parameter value redir_class “redirect”`	Applies redirect rules to the subscriber traffic.
	Specify a service condition for the pass service profile and its default condition.	`parameter value pass_class “pass”`	Applies pass rules to the subscriber traffic.
	Specify a service condition for the drop service profile and its default condition.	`parameter value drop_class “drop”`	Applies drop rules to the subscriber traffic.
	Assign the class from the redirect parameters to the appropriate attribute	`set class`	
	Assign the class from the pass parameters to the appropriate attribute	`set class`	
	Assign the class from the drop parameters to the appropriate attribute	`set class`	
6.	Convert all the rules in HTTP-Redirect-Rule attributes into Dynamic-IP-Filter rules. For general information about specifying attributes for service conditions in a profile, see *Configure a RADIUS-Guided Service Profile* in *Configuring RADIUS* .		

Table 3 Configuring Hotlining Services for an FA

#	Task	Root Command	Notes
	Apply the service policy attribute for incoming traffic .	**attribute** ***attribute-name*** **in** ***attribute-value***	Enter this command to specify an attribute for each service condition in this profile.
	Copy the URL value from the HTTP-Redirect Rule attribute and assign it to HTTP-Redirect-url.	**attribute HTTP-Redirect -url from HTTP-Redirect-Rule url**	
	Extract the IP filter rules present in the HTTP-Redirect-Rules and convert them to Dynamic-IP-Filter rules.	**attribute Dynamic-IP-Filter from HTTP-Redirect-Rule**	If you do not want to drop nonconforming HTTP traffic, then this line should be removed from the RSE profile configuration.
	Adds more IP filters as desired.	**attribute** [**vendor-specific** {**rbak** | ***vendor-num***}] {***attribute-name*** | ***attribute-num***} **drop** [***msg-type-1... msg-type-n***]	Repeat this step to add as many IP filters as desired. If you do not want to drop non-confirming HTTP traffic then this line should be removed from the RSE profile configuration.
7.	Map the RADIUS service profile to MIP FA subscribers.		
	Specify the default subscriber and access subscriber configuration mode.	**subscriber default**	Enter this command in context configuration mode.
	Specify the RSE profile that references the policy that defines the classes to which you want to map the HTTP redirect rules.	**service profile hotline** ***profile-name***	This command maps the HTTP redirect rules to classes defined in the policy that is referenced in the specified RSE profile for a MIP FA subscriber.
8.	Enable the sending of the NAS IP Address attribute in RADIUS packets. For more information about configuring and sending attributes RADIUS packets, see *Configure and Send Attributes in RADIUS Packets (Optional)* in *Configuring RADIUS* .		
	Include the NAS IP Address attribute in the RADIUS Access-Request and Accounting-Request packets sent by the SmartEdge router.	**radius attribute NAS_IP_Address interface** ***if-name***	Enter this command in context configuration mode. Replace the ***if-name*** argument with the name of the interface whose primary IP address you want use as the source IP address sent in RADIUS packets. Note that, if the interface is not configured or is unreachable, the IP address of the outgoing interface is used instead as the source IP address for packets.

Table 3 Configuring Hotlining Services for an FA

#	Task	Root Command	Notes
9.	Enable the forwarding of nonmobile IP traffic for the FA to prevent traffic leaks. For general information about configuring an FA, see `Mobile IP Foreign Agent`.		
	Access Mobile IP configuration mode.	**`router mobile-ip`**	Enter this command in context configuration mode.
	Select the FA instance in this context and access FA configuration mode.	**`foreign-agent`**	
10.	On the RADIUS server, configure the forward policy to intercept incoming packets by default. For more information, see the appropriate RADIUS documentation.		

3 Configuration Examples

The following example shows how to configure hotlining for an FA on a SmartEdge router that is acting as an ASN-GW EP in a WiMAX network:

```
! Configure a local 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 server. All the hotlining rules are received from
R7 interface or the RADIUS server:

[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#radius server 10.12.209.3 encrypted-key
3828082561D6BDD6

! Configure the accounting server. This configuration is used if the
accounting_mode is set for the subscriber:

[local]Redback(config-ctx)#radius accounting server 1.1.1.1 key redback
[local]Redback(config-ctx)#aaa accounting subscriber radius
attribute-guided

! Configure the CoA server so that AAAd will accept CoA messages from the
configured server only

[local]Redback(config-ctx)# radius coa server 2.2.2.2 key 1234567

! Configure a RADIUS guided Forward policy with pass, redirect and drop
 classes.

[local]Redback(config)#forward policy captive-portal radius-guided
[local]Redback(config-policy-frwd)#access-group
[local]Redback(config-policy-frwd)#class redirect
[local]Redback(config-policy-frwd)#redirect destination local
[local]Redback(config-policy-frwd)#class pass
[local]Redback(config-policy-frwd)#class drop
[local]Redback(config-policy-frwd)#drop

! Configure the RADIUS service profile with the forward policy to apply
HTTP redirect rules:

[local]Redback(config)# context local
[local]Redback(config-ctx)# radius service profile WIMAX-HTTP-Redirect
[local]Redback(config-service-profile)# parameter value redir_class
```

```
“redirect”
[local]Redback(config-service-profile)# parameter value pass_class
“pass”

! Set the class name from the given parameters to the appropriate attributes:

[local]Redback(config-service-profile)# set class $redir_class
HTTP-Redirect-Rule redirect
[local]Redback(config-service-profile)# set class $pass_class
HTTP-Redirect-Rule pass

!Apply the Captive-Portal forward policy to incoming traffic:

[local]Redback(config-service-profile)# attribute Forward-Policy in
Captive-Portal

!Copy the URL value from HTTP-Redirect-Rule and assign it to
HTTP-Redirect-url:

[local]Redback(config-service-profile)#attribute HTTP-Redirect-url from
HTTP-Redirect-Rule url

!Convert all the rules in HTTP-Redirect-Rule into Dynamic-IP-Filter rules:

[local]Redback(config-service-profile)#attribute Dynamic-IP-Filter from
HTTP-Redirect-Rule
[local]Redback(config-service-profile)#attribute Dynamic-IP-Filter "in
6 from any to any 80 class drop fwd"
[local]Redback(config-service-profile)#attribute Dynamic-IP-Filter "in
6 from any to any 8080 class drop fwd"
[local]Redback(config-service-profile)#attribute Dynamic-IP-Filter "in
6 from any to any 443 class drop fwd"
```