ERICSSON

Configuring Mobile IP for a Home Agent

SYSTEM ADMINISTRATOR GUIDE

42/1543-CRA 119 1170/1-V1 Uen D

Contents

1 Overview

1.1 Configuring a Mobile IP Home Agent

This document describes the tasks used to configure Mobile IP wireless services for home-agent (HA) instances on the SmartEdge® router and their foreign-agent (FA) peers. This document also provides a configuration example to support Mobile IP wireless services for an HA instance on the router and its FA peer. Operations tasks for monitoring, administering, and troubleshooting Mobile IP features are also described in this document.

Note: The terms FA instance and HA instance, each refer to the FAs and HAs, respectively, that you configure on the SmartEdge router.

The terms FA peer and HA peer refer to FAs and HAs that exist on other equipment in the network.

The term Mobile IP binding refers to the association between a mobile node (MN) and its HA instance on the SmartEdge router. The term visitor or visiting MN refers to the association between an MN and an FA instance when that MN is communicating with its HA through the FA instance on the SmartEdge router.

HA tunnels can be used with Mobile IP services and non-Mobile IP services traffic.

You configure IP-in-IP and, optionally, Generic Routing Encapsulation (GRE) tunnels on the SmartEdge router to support the connections from FA instances to their HA peers and from HA instances to their FA peers. For information about configuring the IP-in-IP and GRE tunnels, see *Configuring Single Circuit Tunnels*.

For information about configuring Ethernet, Fast Ethernet-Gigabit Ethernet, and Gigabit Ethernet ports and circuits to support mobile subscribers, see *Configuring ATM, Ethernet, and POS Ports* and *Configuring Circuits*.

1.2 Traffic Flow

Mobile IP services allows MNs to retain their IP addresses, and therefore maintain their existing IP sessions, when they roam across multiple networks.

Mobile IP consists of the following components:

- MNs
- HA instance

- FA peer

The HA instance, a router on the MN home network, is the anchor component in Mobile IP network that provides seamless mobility to the MN. When an MN is attached to its home network, it does not use Mobile IP services because it communicates directly using normal IP routing. When a MN is roaming and is not connected to its home network, its HA instance:

- Tracks the MN current point of attachment (POA) to the Internet.
- Tunnels datagrams destined to the MN current POA. HA tunnels can be used with Mobile IP services and non-Mobile IP services traffic.
- Authenticates the MN (usually with the user ID and password) and verifies that IP Mobile services should be provided. It optionally assigns the MN a home address (HoA) on its home network. When the MN roams outside its home network, it can retain its home address so that active IP sessions remain up, or can have an address dynamically assigned to it by the CAPC or AAA server.
- Receives reverse-tunneled packets from the FA peer and forwards them based on the IP packet sent by MN.

Mobile IP services enable the SmartEdge router to act as one or more HA instances. Each instance communicates with its mobile subscribers (MNs). When an MN moves outside the network for the HA instance, it connects to the HA instance through an FA peer, which then communicates with the HA instance. Each HA instance has a local address that the system uses as the termination address for its MNs and FA peers.

Mobile IP subscribers are assigned a home slot where their corresponding subscriber circuit is anchored for the purposes of accounting and other circuit-based features. When selecting a home slot, preference is given to the line card with the current HA-FA tunnel egress circuit. When a subscriber reregisters and the subscriber's home slot is not on the same line card as the tunnel egress, an attempt will be made to reoptimize the subscriber's home slot.

In a typical deployment, MNs connect wirelessly to Base Transceiver Stations (BTSs), which connect to the SmartEdge router FA peer through Ethernet. In this topology, each MN is represented by a separate Ethernet circuit and MNs can move between BTSs. The FA instance communicates with a SmartEdge HA instance through a tunnel endpoint (a local address of an HA instance). The SmartEdge router routes the MN traffic to the FA peer using an IP-in-IP tunnel or GRE tunnel. Each FA peer uses a different tunnel. Traffic for the MNs is routed from the HA instance to the FA peer using the same tunnel.

Note: Because the tunnels described in this document each support a single tunnel circuit, the term tunnel refers to the tunnel and its circuit. For information about configuring the IP-in-IP and GRE tunnels, see *Configuring Single Circuit Tunnels*.

Figure 1 illustrates the physical network of MNs, BTS, FA peers, and an HA instance.

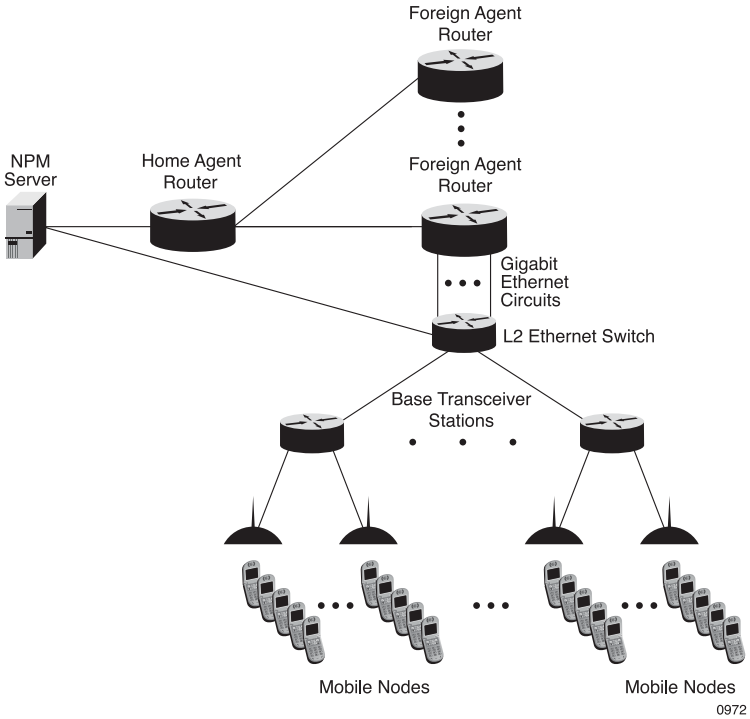

Figure 1 Physical Network of MNs, BTS, FA peers, and an HA Instance

1.3 Deployment Scenarios

The Mobile IP services implementation can use the SmartEdge OS multiple context support. For the HA, all home addresses (HoAs) are allocated from the HA context address space. The HA local address interfaces can be in the same context or in different contexts. This allows IP-in-IP or GRE tunnels to FA peers to terminate in other contexts. For example, an FA peer tunnel could terminate in the local context that is providing connectivity to the Internet backbone.

1.4 Restrictions

Mobile IP services is currently supported only for unicast traffic; broadcast and multicast traffic are not supported.

Mobile IP services is supported only on PPA2 line cards. Do not install any PPA1-based line cards on the chassis when enabling Mobile IP Services.

1.5 Supported Standards

Mobile IP services comply with the standards in the following documents:

- RFC 2794—*Mobile IP Network Access Identifier Extension for IPv4*
- RFC 3024—*Reverse Tunneling for Mobile IP, revised*
- RFC 3344—*IP Mobility Support for IPv4*
- RFC 3543—*Registration Revocation in Mobile IPv4*
- X.S0011-001-C v3.0, *cdma2000 Wireless IP Network Standard: Introduction*
- RFC 4433—*Mobile IPv4 Dynamic Home Agent (HA) Assignment*

2 Configuration and Operations Tasks

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

To configure HA Mobile IP features, perform the tasks described in the following sections:

2.1 Mobile IP Configuration Guidelines

The following HA configuration guidelines apply when configuring Mobile IP services for an HA instance:

- Within a given context, the SmartEdge router can act as an HA instance or an FA instance; it cannot perform both roles. For information about configuring it as an FA instance, see *Configuring ANCP*.
- You must configure IP-in-IP tunnels to FA peers; optionally, you can configure and use GRE tunnels in addition to the IP-in-IP tunnels.
- Configure the tunnel to an FA peer in the HA context for that peer.
- MNs do not connect directly with an HA instance; instead they reach that HA instance through its FA peers. If the SmartEdge router is also acting as an FA instance (in another context), the MNs can connect to that FA instance as described in *Configuring Mobile IP for a Foreign Agent*.
- To prevent Mobile IP tunnels from shutting down because of circuit problems, create the interfaces for the IP-in-IP and GRE tunnels as loopback interfaces. Loopback interfaces are always up.
- When using GRE tunnels to connect FA peers, a separate GRE tunnel is required for each FA peer. GRE keys are not supported.

2.2 Create the Contexts and Interfaces for Mobile IP Services

To create the contexts and interfaces for Mobile IP services, perform the tasks described in Table 1. These contexts and interfaces are used in subsequent configuration tasks for the HA instances and FA peers.

Table 1 Create the Contexts and Interfaces for Mobile IP Services

#	Task	Root Command	Notes
1.	Optional. Create the context for the HA instance and access context configuration mode.	*context*	Enter this command in global configuration mode. You can use the local context instead of performing this step.
2.	Create an interface for the FA peers to connect to the HA instance (using tunnels) using the HA local address and access interface configuration mode.	*interface*	Enter this command in context configuration mode.
3.	Optional. Create an FA context for an FA peer and access context configuration mode.	*context*	Enter this command in global configuration mode. You can use the HA instance context for all FA peers instead of performing this step.

Note: For information about the context command (in global configuration mode) and the interface command (in context configuration mode), and the various commands to configure contexts and interfaces, see *Configuring Contexts and Interfaces*.

2.3 Configure a Key Chain for FA-HA Authentication

To configure a key chain authentication for the FA and HA, perform the tasks described in Table 2. For more information about configuring key chains, see *Configuring Bridging*.

Table 2 Configure a Key Chain

#	Task	Root Command	Notes
1.	Select the context for the HA instance and access context configuration mode.	*context*	Enter this command in global configuration mode.
2.	Create the key chain and access key chain configuration mode.	*key-chain*	Enter this command in context configuration mode.
3.	Configure a key string.	*key-string*	Enter this command in key chain configuration mode.
4.	Specify the security parameter index (SPI) for this key chain.	*spi*	Enter this command in key chain configuration mode.

2.4 Configure an HA Instance

To configure an HA instance, perform the tasks described in Table 3; enter all commands in HA configuration mode, unless otherwise noted.

Table 3 Configure an HA Instance

#	Task	Root Command	Notes
1.	Select the context for the HA instance and access context configuration mode.	*context*	Enter this command in global configuration mode.
2.	Enable Mobile IP services in this context and access Mobile IP configuration mode.	*router mobile-ip*	Enter this command in context configuration mode.
3.	Create or select the HA instance and access HA configuration mode.	*home-agent*	Enter this command in Mobile IP configuration mode.
4.	Apply a dynamic tunnel profile to an HA instance.	*dynamic-tunnel-profile*	Enter this command in HA configuration mode.
5.	Specify the interface for the HA local address.	*local-address*	This is the interface that you created for the tunnels for this HA instance.
6.	Optional. Enable the optional tunnel type.	*tunnel-type*	The default is not to enable optional tunnel types.
7.	Optional. Configure the default authentication for this HA instance.	*authentication (home agent instance)*	This is the default authentication for all FA peers for this HA instance.
8.	Optional. Configure the registration maximum lifetime for MN registrations using this HA instance.	*registration max-lifetime (HA)*	The default is 1800 seconds.
9.	Optional. Configure the tolerance for timestamp-based replay protection between an MN and its HA instance.	*replay-tolerance*	The default is 7 seconds.
10.	Optional. Configure registration revocation support for this HA instance.	*revocation (HA)*	The default is that registration revocation is not enabled.

2.5 Configure an FA Peer

To configure an FA peer, perform the tasks described in Table 4.

Table 4 Configure an FA Peer

#	Task	Root Command	Notes
1.	Select the context for the HA instance for this FA peer and access context configuration mode.	*context*	Enter this command in global configuration mode.
2.	Enable Mobile IP services in this context and access Mobile IP configuration mode.	*router mobile-ip*	Enter this command in context configuration mode.
3.	Select the HA instance for the FA peer and access HA configuration mode.	*home-agent*	Enter this command in Mobile IP configuration mode.
4.	Create or select the FA peer and access FA peer configuration mode.	*foreign-agent-peer*	Enter this command in HA configuration mode.
5.	Optional. Apply a dynamic tunnel profile to an FA peer.	*dynamic-tunnel-profile*	Enter this command in FA peer configuration mode. The dynamic tunnel profile is created in Mobile IP configuration and Dynamic Tunnel Profile configuration mode.
6.	Optional. Configure the authentication for the FA peer.	*authentication (home agent instance)*	Enter this command in FA peer configuration mode. This authentication overrides the default authentication for all FA peers for this HA instance.

2.6 Configure an MN Subscriber

To configure an MN subscriber record, profile, or default profile, perform the task described in Table 5.

Table 5 Configure an MN Subscriber Record, Profile, or Default Profile

#	Task	Root Command	Notes
1.	Configure the subscriber record, profile, or default profile.	*subscriber*	For information about configuring subscribers and their attributes, see *Configuring Subscribers*.

2.7 Configure AAA for MN Subscribers

You can configure authentication, authorization, and accounting (AAA) features and Remote Authentication Dial-In User Service (RADIUS) servers for MN subscribers. For information about configuring AAA features, see *Configuring Bridging* and *Configuring RADIUS*.

2.8 Configure the Mobile IP Tunnels

You must configure an IP-in-IP tunnel to each FA peer. You can also configure a GRE tunnel to each FA peer. To configure the Mobile IP tunnels, perform the tasks described in Table 6.

Table 6 Configure the Mobile IP Tunnels

#	Task	Root Command	Notes
1.	Configure the IP-in-IP tunnels to the FA peers.		For information about creating IP-in-IP tunnels and GRE tunnels, see *Configuring GRE Tunnels*.
2.	Optional. Configure the GRE tunnels to the FA peers.		For information about creating IP-in-IP tunnels and GRE tunnels, see *Configuring Single Circuit Tunnels*.

2.9 Enable or Disable an HA Instance or FA Peer

To enable or disable an HA instance or an FA peer, perform the task described in Table 7.

Table 7 Enable or Disable an FA, an HA Peer, or MN Access to the SmartEdge Router

Task	Root Command	Notes
Optional. Disable or enable an HA instance or an FA peer.	*shutdown (Mobile IP)*	Enter this command in HA instance or FA peer interface configuration mode. Use the **no** form of this command to enable an HA instance or an FA peer.

2.10 Operations Tasks

To monitor, administer, and troubleshoot Mobile IP features, perform the appropriate task listed in Table 8. Enter the **clear** and **debug** commands in exec mode; enter all **show** commands in any mode.

Note: All **show** commands for Mobile IP services, with the exception of the **show mobile-ip** all command, display information for the current context.

Table 8 Mobile IP Operations Tasks

Task	Root Command
Clear the mobile node (MN) binding.	*clear mobile-ip binding*

Table 8 Mobile IP Operations Tasks

Task	Root Command
Clear Mobile IP counters for an FA instance and HA instance.	*clear mobile-ip counters*
Clear Mobile IP dynamic FA-HA authentication keys corresponding to the specified HA peer, FA peer, or HA local-address.	*clear mobile-ip dynamic-keys*
Clear FA peer information or only FA peer counters on an HA instance.	*clear mobile-ip foreign-agent-pe er*
Clear HA peer information or only HA peer counters on an FA instance.	*clear mobile-ip home-agent-peer*
Clear the FA instance access interface, including all Mobile-IP visitors associated with the access interface or FA access interface counters.	*clear mobile-ip interface*
Clear one or more visitors to an FA instance.	*clear mobile-ip visitor*
Clear all Mobile IP subscribers in the current context or all contexts.	*clear subscriber encapsulation mobile-ip*
Enable the generation of debug messages for Mobile IP services on a circuit.	*debug circuit mobile-ip*
Enable the generation of debug messages for the specified type of Mobile IP events.	*debug mobile-ip*
Enable the generation of debug messages for an HA instance and FA instance.	*debug mobile-ip agent-common*
Enable the generation of debug messages for Mobile IP authentication.	*debug mobile-ip authentication*
Enable the generation of debug messages for an FA instance.	*debug mobile-ip foreign-agent*
Enable the generation of debug messages for an HA instance.	*debug mobile-ip home-agent*
Enable the generation of debug messages for Mobile IP module interaction events, such as Router Configuration Manager (RCM) events and Interface and Circuit State Manager (ISM).	*debug mobile-ip interaction*
Enable the generation of debug messages for the specified type of Mobile IP packets. This is a filtered debugging feature for specific source, destination, circuit, or packet types.	*debug mobile-ip packet*
Enable the generation of debug messages for Mobile IP I/O packet events on a kernel socket interface.	*debug mobile-ip packet-io*

Table 8 Mobile IP Operations Tasks

Task	Root Command
Enable the generation of subscriber debug messages on Mobile IP service user name events on an HA instance.	*debug subscriber*
Display the Mobile IP configuration.	*show configuration mobile-ip*
Display IP routes for MNs.	*show ip route mobile-ip*
Display Mobile IP information for one or more contexts.	*show mobile-ip*
Display Mobile IP binding information for one or all FA peers for an HA instance.	*Fields Displayed by the show nd neighbor Command*
Display Mobile IP pending visitor registration information for FA peers or for an HA instance.	*show mobile-ip binding pending*
Display Mobile IP information for care-of address (CoA) information for an FA instance.	*show mobile-ip care-of-address*
Display Mobile IP debug settings.	*show mobile-ip debug*
Display WiMAX dynamic authentication keys used by an HA or FA instance.	*show mobile-ip dynamic-key*
Display information about dynamic tunnel profiles.	*show mobile-ip dynamic-tunnel -profile*
Display Mobile IP information for one or all FA peers for an HA instance.	*show mobile-ip foreign-agent-p eer*
Display Mobile IP information for one or all HA peers for an FA instance.	*show mobile-ip home-agent-peer*
Display information for one or more Mobile IP interfaces.	*show mobile-ip interface*
Display HA local address information for the specified interface or all local address interfaces for the HA instance.	*show mobile-ip local-address*
Display log information for authentication, authorization, and accounting (AAA), ISM events, and malformed packets.	*show mobile-ip log*
Display Mobile IP tunnel statistics.	*show mobile-ip statistics tunnel*
Display information about static and dynamic tunnels registered with Mobile IP services.	*show mobile-ip tunnel*
Display a list of Mobile IP visitors to an FA instance.	*show mobile-ip visitor*
Display a list of pending Mobile IP visitors to an FA instance.	*show mobile-ip visitor pending*

3 Configuration Examples

The following example creates an IP-in-IP tunnel and the interfaces to support an HA instance and an FA peer, all in the local context. Traffic is carried on two Ethernet ports:

```
[local]Redback(config)#context
[local]Redback(config)#context local

!Create the interfaces for the IP-in-IP tunnels to the FA peers and for
the MNs

[local]Redback(config)#context local
[local]Redback(config-ctx)#interface tun1
[local]Redback(config-if)#ip address 20.2.1.1/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface loc-addr
[local]Redback(config-if)#ip address 20.1.1.1/16
[local]Redback(config-if)#exit

!Enable the local context for Mobile IP services

[local]Redback(config-ctx)#router mobile-ip

!Create the home agent instance, specify the local address interface
and create a foreign agent peer

[local]Redback(config-mip)#home-agent
[local]Redback(config-mip-fa)#local-address loc-addr
[local]Redback(config-mip-fa)#foreign-agent-peer 20.1.1.2
[local]Redback(config-mip-hapeer)#end

!Configure the Ethernet circuits (bind them to the MN access and
local address interfaces)

[local]Redback#config
[local]Redback(config)#port ethernet 2/10
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#port ethernet 2/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface loc-addr local
[local]Redback(config-port)#exit

!Configure the IP-in-IP tunnel (bind it to the tunnel interface in the
local context)

[local]Redback(config)#tunnel ipip tun1
[local]Redback(config-tunnel)#peer-end-point local 20.1.1.1 remote 20.1.1.2
[local]Redback(config-tunnel)#bind interface tun1 local
[local]Redback(config-tunnel)#end
```