ERICSSON

Configuring Mobile IP for a Foreign Agent

SYSTEM ADMINISTRATOR GUIDE

41/1543-CRA 119 1170/1-V1 Uen F

Contents

1 Overview

This document describes the tasks used to configure SmartEdge® OS Mobile IP wireless services for foreign agent (FA) instances on the SmartEdge router and their home agent (HA) peers. This document also provides configuration examples to support Mobile IP wireless services for FA instances on the router and their 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 refer to the FAs and HAs, respectively, that you configure on the SmartEdge router.

The terms FA peers and HA peers 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.

Generic Routing Encapsulation (GRE) and IP-in-IP tunnels can be used with Mobile IP services and nonmobile IP services traffic.

You can configure IP-in-IP tunnels and, optionally, 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, 802.3 ad access link group, Fast Ethernet-Gigabit Ethernet, and Gigabit Ethernet ports and circuits to support mobile subscribers, see *Configuring ATM, Ethernet, and POS Ports* and *Configuring Circuits*.

1.1 Mobile IP Components

Mobile IP allows MNs to retain their IP addresses when they roam across multiple networks. Doing so enables MNs to maintain their existing IP sessions.

Mobile IP consists of the following components:

- Mobile Nodes
- Home Agent Peer
- Foreign Agent Instance

- Registration

1.1.1 Mobile Nodes

The MN is an IP device—for example, a laptop computer or personal digital assistant (PDA)—whose point of attachment (POA) to the Internet can frequently change. The MN maintains its connections by using its home IP address.

1.1.2 Home Agent Peer

The HA peer, 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 an MN is roaming and is not connected to its home network, its HA peer does the following:

- Tracks the MN current POA to the Internet.
- Tunnels datagrams destined to the MN current POA.
- Authenticates the MN (usually with the user ID and password) and verifies that IP Mobile services are provided. It optionally assigns the MN a home address (HoA) on its home network. When the MN roams outside its home network, it retains its home address to prevent losing existing IP sessions.

1.1.3 Foreign Agent Instance

MNs listen for FA instance advertisements to determine if they are attached to a home or foreign network. An FA instance is a router on a foreign network that provides routing services to visiting MNs. When the MN visits a foreign network with which its HA peer has service agreements and is authenticated by its HA peer, the MN can obtain Mobile IP services while visiting this network. During the visit, the MN listens for Internet Control Message Protocol (ICMP) router advertisements (RAs) from an FA instance. The RAs allow the MN to learn which FA instances are available and what Mobile IP services they have to provide. The FA instance does the following:

- Allows the MN to maintain its existing sessions when it visits the foreign network.
- Terminates the tunnels from HAs peers corresponding to visiting MNs.
- Decapsulates packets destined for the MN and delivers them locally.
- Reverse-tunnels traffic from the MN to other Internet nodes, which is often required to satisfy ingress filtering (as described in RFC 2827, `Network Ingress Filtering: Defeating Denial of Service Attacks`) and facilitate accurate billing and accounting.

If the MN does not hear RAs from any FAs, the MN sends an ICMP router solicitation requesting that any FA instances on the foreign network reply with an RA.

1.1.4 Registration

When the MN discovers a foreign agent (FA) instance with which its HA peer has a service agreement, it sends a Mobile IP registration request to the FA instance. The FA instance validates the request and forwards it to the corresponding HA peer. The registration request does the following:

- Requests Mobile IP services for the MN from the FA instance when it is visiting one of its foreign networks. For successful registrations, the FA instance maintains the state of the visitor, such as the lifetime of the registration.
- Informs the HA peer of the MN current POA to the Internet. This POA is normally the FA instance care-of-address (CoA), which is also the termination point of the tunnel between the HA peer and FA instance.
- For new registrations, the HA peer creates a binding that maintains the MN location and other related information, such as the lifetime of the registration. For existing registrations, the HA peer and FA instance renews the registration lifetime in their respective binding and visitor entries.
- Optionally, deregisters the MN when it returns to its home network or no longer requires Mobile IP services.

The MN registration request includes the FA instance CoA and the IP address of its HA peer. It may include the MN assigned home address (HoA) and the MN user identity as described in *RFC 2794, Mobile IP Network Access Identifier Extension for IPv4s*, or an MN-FA authentication extension as described in *RFC 3344 IP Mobility Support for IPv4*, or a dynamic home agent extension as described in *RFC 4433 Mobile IPv4 Dynamic Home Agent (HA) Assignment*. In dynamic HA assignment, the HA IP address in the registration request can be 0.0.0.0 or 255.255.255.255..

The MN sends the registration request to the HA peer so that the HA peer knows where the MN is located. When the MN is successfully authenticated, the HA peer sends a Mobile IP registration reply to the FA instance and the FA instance, in turn, forwards it to the MN.

The HA peer and FA instance also set up forwarding so that all packets destined for the MN home address are forwarded to the MN through the tunnel between the HA peer and the FA instance. The FA instance sets up forwarding so that packets from the MN are reverse tunneled to back over the same tunnel to the HA peer. Packets originating from an MN are always reverse tunneled.

The MN uses its HoA as the source of all packets it sends when it is attached to its home network or visits a foreign network through an FA instance. MN authentication is always performed on the HA peer. The SmartEdge router

HA peer employs the user identifier of the MN (included in the registration request) to authenticate mobile IP services that are using AAA protocols with a RADIUS server.

Optionally, the MN can acquire a collocated care-of address (CCoA) on the foreign network and perform Mobile IP services without, or with minimal interaction, with the FA instance. The SmartEdge router does not support this mode of operation.

1.2 Traffic Flow

Mobile IP services enables the SmartEdge router to act as one or more FA instances. Each FA instance communicates with HA peers that support its mobile subscribers, which are referred to as mobile nodes (MNs). Each FA instance has a care-of address (CoA) that the system uses as the termination address for the tunnel to an HA peer.

In a typical deployment, MNs connect wirelessly to base transceiver stations (BTSs), which connect to the SmartEdge router FA instance 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 peer through a tunnel endpoint (a local address of an HA instance). The SmartEdge router routes the MN traffic to the HA peer by using an IP-in-IP tunnel or GRE tunnel. Each HA peer uses a different tunnel. Traffic for the MNs is routed from the FA instance to the HA peer through the same tunnel.

MNs communicate with the SmartEdge router (the FA instance) over Ethernet-based circuits using a context where you configure the FA instance. The system routes the MN traffic to each external HA peer using an IP-in-IP tunnel or a GRE tunnel. Each HA peer uses a different tunnel. Traffic from an HA peer is routed back to the MNs associated with that HA 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 for MNs, BTS, HA peers, and an FA instance.

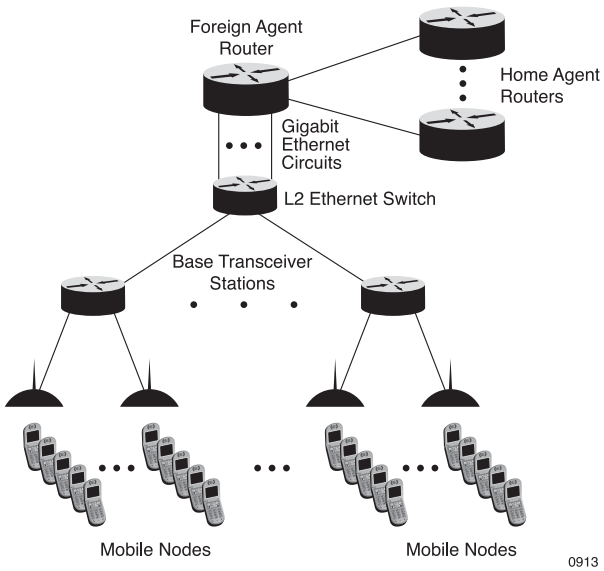

Figure 1 Physical Network of MNs, BTSs, HA Peers, and an FA Instance

1.3 Subscriber Services

A subscriber circuit is associated with each MN attached to an FA. Application of circuit-based services to MNs attached to FA currently is limited to hotlining. For information on hotlining, see *Configuring Hotlining for a Foreign Agent*.

Each FA subscriber circuit is associated with the Layer 2 access circuit through which the MN connects to the FA. The access circuit may change due to mobility events. The FA subscriber circuit is typically created on the same physical slot as the access circuit. If sufficient capacity is not available on that slot, an alternate slot is chosen. The physical card slot on which the FA subscriber circuit gets created is referred to as the home slot for the subscriber. The home slot does not change as a result of mobility events. If the home slot fails, the FA subscriber circuit is created on an alternate slot.

If an XCRP controller card is switched over or the Mobile IP process is restarted, the MN visitor entries are recovered from shared memory and data forwarding continues uninterrupted.

Subscriber services provided by the SmartEdge FAs attached to MNs are subject to the following requirements and restrictions:

- Subscriber services must be configured on RADIUS. The only service supported on FAs is hotlining. See *Configuring Hotlining for a Foreign Agent* for more information about hotlining for an FA. Other services such as QoS, ACLs are not supported. By default, RADIUS is used for authenticating the MNs on the FA. If the RADIUS server is not configured, the MN sessions do not come up. If hotlining services are not required, you must use the **`aaa subscriber authentication none`** command in the FA context to disable RADIUS authentication.

- The FA context and each of the VPN contexts (if any) associated with the HA peers must be configured with a multibind last-resort interface.

- MN visitor entries are saved in shared memory only for those MNs that have successfully completed the registration process on both the FA and the HA. Switch over XCRP controller cards preserves MN visitor sessions only if the MN has completed session registration.

- An NAI (network address identifier) is required in Mobile IP registrations.

1.4 Deployment Scenarios

The Mobile IP services implementation can use the multiple context support that the SmartEdge OS provides. The contexts that Mobile IP services can use in different deployment scenarios include:

- CoA context

  The CoA interface resides in the CoA context. The CoA interface provides an endpoint for a tunnel to a home-agent peer. The CoA context is typically the local context, but other contexts can be used as well. Each CoA interface can be in a different CoA context independent of other CoA interfaces.

- FA context

  The FA context provides one or more interfaces to the MN and defines the set of HA peers for the FA instance. Each FA instance configured on the SmartEdge router has its own FA context.

- HoA VPN context

  The home address (HoA) Virtual Private Network (VPN) context includes the interfaces that terminate the tunnels to the HA peers. Each HA peer that uses private HoAs has its own context. HA peers that use non-overlapping HoAs can share a single context. Each HA peer that has an overlapping HoA must have its own HoA VPN context.

These contexts allow the SmartEdge OS to support various deployment scenarios, which are described in the following sections:

1.4.1 Home Agent Without Overlapping IP Addresses

In the most basic deployment, a single FA instance provides connectivity to all MNs while interfacing with all the HA peers. The MN HoAs do not overlap; that is, each MN has a public HoA. In this case, the configuration is simplified to make use of a single context, the FA context.

1.4.2 Some Home Agents Use Private IP Addresses

A few HA peers can allocate HoAs from a private address space while providing Internet connectivity using Network Address Translation (NAT). If so, the IP addresses of the MNs can overlap.

To configure the SmartEdge OS for this deployment, use a single context for the FA instances, HA peers, and CoAs, but exclude the HA peers that use private IP addresses. Use a separate context for each HA peer that uses a private address space.

1.4.3 Any Home Agent Can Use Private IP Addresses

Each HA peer is independent and can use private IP addresses. For this deployment scenario, each HA peer uses a separate context. The CoA and FA contexts can be the same.

1.4.4 Home Agents Can Be Grouped for Each Mobile IP Service Provider

In this scenario, an FA instance provides services to multiple mobile Internet service providers (ISPs). Each ISP owns a set of HA peers and the HoAs that belong to the same ISP do not overlap. Each ISP may use private IP addresses.

To configure this scenario, each ISP uses a separate HoA VPN context; that is, all HA peers belonging to an ISP use the same HoA VPN context. The CoA and FA contexts can be the same for each ISP.

1.4.5 Wholesale Mobile IP Services for Other Providers

In this scenario, the SmartEdge OS can separate MN, FA, and HA peer networks for each mobile ISP. Each ISP is like an enterprise VPN, ISP contexts are as follows:

- A separate FA context is used for each ISP.
- The CoA context for each ISP can be the same as its FA context; this is more appropriate than using the local context because the ISP can choose to use private IP addresses for the tunnel endpoints.
- The FA context can also serve as the HoA VPN context, assuming that no HoAs overlap within the same ISP. If HoAs overlap, then a separate HoA VPN context is used for each HoA peer.

If the backbone links are not within a nonlocal context, then the backbone connectivity is through the local context.

1.5 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.

1.6 Supported Standards

Mobile IP services comply with the standards found 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***
- 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 FA instances on the SmartEdge router and their home-agent (HA) peers, use the configuration guidelines and perform the tasks described in the following sections:

2.1 Mobile IP Configuration Guidelines

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

- Within a given context, the SmartEdge router can act as an HA instance or an FA instance.
- HA peers that use public IP addresses can share an HoA VPN context.
- If an HA peer uses private IP addresses, it can share an HoA VPN context with other HA peers if their IP addresses do not overlap; otherwise, HA peers cannot share a HoA VPN context.
- MNs can have overlapping IP addresses if they are registered with different HA peers.
- You must configure IP-in-IP tunnels to HA peers; optionally, you can configure and use GRE tunnels in addition to the IP-in-IP tunnels.
- Configure the tunnel to an HA peer in the HoA VPN context for that peer if it exists; otherwise, configure the tunnel in the FA context (the default for the HoA VPN context for that peer).
- 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 you configure the Ethernet circuits that provide access for all MNs, create a single interface in the FA context for all the Ethernet circuits or create a separate interface in the FA context for each 802.1Q permanent virtual circuit (VLAN) or 802.3ad access link group circuit in economical mode.
- FA Subscribers are supported over 802.3 ad access link groups in economical mode only. Note that FA subscribers are not supported over 802.3 ad access link Groups in hitless mode.
- Access link groups that are not configured in economical mode do not support Mobile IP services.

- If Mobile IP services are enabled on a VLAN in an 802.3ad access link group, no other service is supported on that VLAN. A single access link group can support multiple services as long as each service is enabled on a different VLAN within the link group.

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 FA instances, HA peers, and Mobile IP tunnels.

Table 1 Create the Contexts and Interfaces for Mobile IP Services

#	Task	Root Command	Notes
1.	Optional. Create the context for the CoA interface and access context configuration mode.	*context*	Enter this command in global configuration mode. You can use the local context instead of performing this step. For information about the context command (in global configuration mode), see *Configuring Contexts and Interfaces*.
2.	Create the CoA interface and access interface configuration mode.	*interface*	Enter this command in context configuration mode. For information about the interface command (in context configuration mode), see *Configuring Contexts and Interfaces*.
3.	Optional. Create an FA context for an FA 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.
4.	Create the interface for the Ethernet ports and 802.1Q VLANs that BTS MNs use to access this FA instance and access interface configuration mode.	*interface*	Enter this command in context configuration mode.(1)
5.	Optional. Create an interface for an IP-in-IP tunnel and, optionally, an interface for a GRE tunnel to the HA peer, and access interface configuration mode.	*interface*	Enter this command in context configuration mode. Consider making this interface a loopback interface.(2)
6.	Create a multibind last-resort interface to which the FA subscriber circuit will be bound and access interface configuration mode.	*interface*	Use the **`interface`** ***`ifname`*** **`multibind lastresort`** syntax. (3)

Table 1 Create the Contexts and Interfaces for Mobile IP Services

#	Task	Root Command	Notes
7.	Enable IP processing on an interface without assigning an explicit IP address to it.	*ip unnumbered*	Use the **ip unnumbered** ***if-name*** syntax. The interface must be configured as an unnumbered interface.(4)
8.	Optional. Create an HoA VPN context for the terminating interfaces for the IP-in IP tunnel and, optionally, a GRE tunnel for one or more HA peers and access context configuration mode.	*context*	Enter this command in global configuration mode. You can use the local context instead of performing this step, but only HA peers that use public IP addresses or non-overlapping private IP addresses can share a single context.
9.	Optional. Create an interface for an IP-in-IP tunnel and, optionally, an interface for a GRE tunnel to the HA peer and access interface configuration mode.	*interface*	Enter this command in context configuration mode. Consider making this interface a loopback interface.(5)
10.	Create a multibind last-resort interface to which the FA subscriber circuit will be bound and access interface configuration mode.	*interface*	Use the **interface** ***ifname*** **multibind lastresort** syntax. (6)
11.	Enable IP processing on an interface without assigning an explicit IP address to it.	*ip unnumbered*	Use the **ip unnumbered** ***if-name*** syntax. The interface must be configured as unnumbered.(7)
12.	Exit interface configuration mode and access context configuration mode.	*exit*	

Table 1 Create the Contexts and Interfaces for Mobile IP Services

#	Task	Root Command	Notes
13.	Optional. Disable RADIUS authentication if services such as hotlining or other subscriber-based services are not used.	*aaa authentication subscriber*	Use the **aaa authentication subscriber none** syntax (8)
14.	Optional. Configure AAA subscriber authentication by Radius servers with IP addresses or host names in the current context.	*aaa authentication subscriber*	Use the **aaa authentication subscriber radius** syntax (9)

(1) This interface can be bound to an Ethernet port, an Ethernet dot1q PVC, or an economical mode access linkgroup.
(2) If you do not complete this step and configure a static tunnel, the Mobile IP process creates tunnels dynamically when required.
(3) Typically, the FA subscriber circuit is bound to the last-resort interface in the FA context. However, if the HoA peer to which the subscriber connects is configured with a VPN context, the subscriber circuit is bound to the last-resort interface in the HoA VPN context. IP-in-IP and GRE tunnels that are dynamically created by the Mobile IP process must also be bound to this interface.
(4) You need to create the interface referred to in the ip unnumbered command. We recommend making this interface a loopback interface.
(5) If you do not complete this step and configure a static tunnel, the Mobile IP process creates tunnels dynamically when required.
(6) Typically, the FA subscriber circuit is bound to the last-resort interface in the FA context. However, if the HoA peer to which the subscriber connects is configured with a VPN context, the subscriber circuit is bound to the last-resort interface in the HoA VPN context. IP-in-IP and GRE tunnels that are dynamically created by the Mobile IP process are also bound to this interface.
(7) You need to create the interface referred to in the ip unnumbered command. We recommend making this interface a loopback interface.
(8) Perform this task only if hotlining is not being used. If hotlining is required, skip this step and perform step 14.
(9) Perform this task only if hotlining is required. If hotlining is not being used, skip this step and perform step 13 only.

2.3 Configure Key Chain Authentication Between an FA and HA

To configure a key chain between a foreign-agent (FA) instance and home-agent (HA) peer, perform the tasks described in Table 2. For more information about configuring key chains, see *Configuring Bridging*. Enter all commands in key chain configuration mode, unless otherwise noted.

Table 2 Configure a Key Chain

#	Task	Root Command	Notes
1.	Select the context for the FA instance and access context configuration mode.	*context*	Enter this command in global configuration mode.

Table 2 Configure a Key Chain

#	Task	Root Command	Notes
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*	
4.	Specify the security parameter index (SPI) for this key chain.	*spi*	

2.4 Configure an FA Instance

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

Table 3 Configure an FA Instance

#	Task	Root Command	Notes
1.	Select the context for the FA 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.	Optional. Create a dynamic tunnel profile and enter Dynamic Tunnel Profile configuration mode.	*dynamic-tunnel-profile*	Enter this command in Mobile IP configuration mode.
4.	Optional. Clear the IP header DF flag in all packets that are transmitted on an IP-in-IP or a GRE tunnel.	*clear-df (dynamic tunnel)*	Enter this command in Dynamic Tunnel Profile configuration mode.
5.	Optional. Set the MTU for packets sent to GRE tunnels.	*gre mtu*	Enter this command in Dynamic Tunnel Profile configuration mode.
6.	Optional. Specify the number of seconds for the router to wait before it brings down a dynamic tunnel that has no active bindings or visitors.	*hold-time*	Enter this command in Dynamic Tunnel Profile configuration mode.
7.	Optional. Set the MTU for packets sent to IP-in-IP tunnels.	*ipip mtu*	Enter this command in Dynamic Tunnel Profile configuration mode.
8.	Optional. Specify the number of seconds for the router to wait for a dynamic tunnel to be established before bringing the current subscriber or visitor down.	*time-out*	Enter this command in Dynamic Tunnel Profile configuration mode.

Table 3 Configure an FA Instance

#	Task	Root Command	Notes
9.	Create or select the FA instance in this context and access FA configuration mode.	*foreign-agent*	
10.	Optional. Reference an existing dynamic tunnel profile. The dynamic tunnel attributes defined in this profile are applied to the dynamic tunnels that are used by this FA instance.	*dynamic-tunnel-profile*	
11.	Specify the interface for the CoA advertised by this FA instance.	*care-of-address*	This is the interface that you created for the tunnel for this FA instance.
12.	Optional. Specify the GRE tunnel type to advertise.	*advertise tunnel-type*	The default is not to advertise optional tunnel types.
13.	Optional. Configure registration revocation.	*revocation (HA)*	The default is to not configure revocation support.
14.	Optional. Configure the default authentication for this FA instance.	*authentication (foreign agent instance)*	This is the default authentication for all HA peers for this FA instance.
15.	Optional. Enable (the default condition) or disable the forwarding of nonmobile IP traffic for this FA instance.	*forwarding traffic*	
16.	Optional. Specifies the means by which the forwarding address for an MN is determined.	*forwarding scheme*	
17.	Optional. Enable or disable MN access interface change detection using logical link control (LLC) exchange ID (XID) messages received on a circuit.	*llc-xid-processing*	Enable is the default.
18.	Optional. Enable or disable optional or mandatory processing of an MN-FA authentication extension.	*authentication mobile-node*	Disable is the default.

2.5 Configure an HA Peer

To configure an HA peer, perform the tasks described in Table 4; enter all commands in HA peer configuration mode, unless otherwise noted.

Table 4 Configure an HA Peer

#	Task	Root Command	Notes
1.	Select the context for the FA instance for this HA 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 FA instance in this context for the HA peer and access FA configuration mode.	*foreign-agent*	Enter this command in Mobile IP configuration mode.
4.	Create or select the HA peer and access HA peer configuration mode.	*home-agent-peer*	Enter this command in FA configuration mode.
5.	Optional. Apply a dynamic tunnel profile.	*dynamic-tunnel-profile*	
6.	Optional. Specify the maximum number of pending registrations for this HA peer.	*max-pending-registrations*	
7.	Optional. Specify the HoA VPN context for this HA peer.	*vpn-context*	This context contains the multibind last resort interface you configured in Section 2.2 on page 10.
8.	Optional. Configure the authentication for the HA peer.	*authentication (foreign agent instance)*	This authentication overrides the default authentication configured for the FA instance.
9.	Exit HA peer configuration mode and access Mobile IP configuration mode.	*exit*	
10.	Exit Mobile IP configuration mode and access context configuration mode.	*exit*	

2.6 Configure a Mobile IP Interface for MN Access

To configure a Mobile IP interface for MN access, perform the tasks described in Table 5; enter all commands in Mobile IP interface configuration mode, unless otherwise noted.

Table 5 Configure a Mobile IP Interface for MN Access

#	Task	Root Command	Notes
1.	Select the context for the FA instance and access context configuration mode.	*context*	Enter this command in global configuration mode.

Table 5 Configure a Mobile IP Interface for MN Access

#	Task	Root Command	Notes
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 an existing interface, enable it for Mobile IP services, and access Mobile IP interface configuration mode.	*interface (mobile IP)*	This interface is the one you created for the Ethernet circuits in step 4 in Table 1.
4.	Optional. Specify the maximum lifetime registration for an MN on this interface.	*registration max-lifetime*	
5.	Optional. Specify the maximum interval between advertisement messages.	*advertise max-interval*	
6.	Optional. Specify the maximum lifetime of advertisement messages.	*advertise max-lifetime*	
7.	Optional. Specify the minimum interval between advertisement messages.	*advertise min-interval*	

2.7 Configure the MN Access to an FA Instance

To configure the MN access to an FA instance, perform the tasks described in Table 6.

Table 6 Configure MN Access to the FA Instance

#	Task	Root Command	Notes
1.	Configure the Ethernet ports and circuits on which the MNs access an FA instance.		For information about configuring Ethernet circuits, see *Configuring ATM, Ethernet, and POS Ports* and *Configuring Circuits*.
2.	Bind the Ethernet ports and circuits to the interfaces created for MN access in the FA context.	*bind interface*	For information about binding circuits to interfaces, see *Configuring Bindings*.

2.8 Configure AAA for MN Subscribers

You can configure AAA features and RADIUS servers for MN subscribers. For information about configuring AAA features, see *Configuring Authentication, Authorization, and Accounting* and *Configuring RADIUS*.

2.9 Configure the Mobile IP Tunnels

You must configure an IP-in-IP tunnel to each HA peer. You can also configure a GRE tunnel to each HA peer. To configure the Mobile IP tunnels, perform the tasks described in Table 7.

Table 7 Configure the Mobile IP Tunnels

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

2.10 Enable or Disable an FA Instance, an HA Peer, or MN Access

To enable or disable an FA instance, an HA peer, or MN access to the SmartEdge router, perform the task described in Table 8.

Table 8 Enable or Disable an FA Instance, an HA Peer, or MN Access to the SmartEdge Router

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

2.11 Operations Tasks

To monitor, administer, and troubleshoot Mobile IP features, perform the appropriate task listed in Table 9. 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 9 Mobile IP Operations Tasks

Task	Root Command
Clear Mobile IP counters for an FA instance.	*clear mobile-ip counters*

Table 9 Mobile IP Operations Tasks

Task	Root Command
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 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 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 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*
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 information for CoA information for an FA instance.	*show mobile-ip care-of-address*
Display Mobile IP debug settings.	*show mobile-ip debug*

Table 9 Mobile IP Operations Tasks

Task	**Root Command**
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 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 log information for 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 examples show configurations for a single FA instance and HA peer with IP-in-IP tunnels, a single FA instance with multiple HA peers and IP-in-IP tunnels, and a link aggregation bundle used as an FA access interface.

3.1 Single FA Instance and HA Peer with IP-in-IP Tunnels

The following example creates an IP-in-IP tunnel and the interfaces to support an FA instance and a single HA peer, all in the local context. The interface for the IP-in-IP tunnel is unnumbered; it borrows its IP address from the CoA interface. Traffic to and from the MNs is carried on GE port **2/1:**

```
! Create the interfaces for the CoA, the MN access, and the IP-in-IP
tunnel to the HA peer, all in the local context

[local]Redback(config)#context local
[local]Redback(config-ctx)#interface coa loopback
[local]Redback(config-if)#ip address 172.16.1.1/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface mn-access
[local]Redback(config-if)#ip address 10.1.1.1/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)# interface loop1 loopback
[local]Redback(config-if)# ip address 192.168.1.1/32
[local]Redback(config-if)# exit
[local]Redback(config-ctx)#interface toHA-peer
[local]Redback(config-if)#ip unnumbered coa
[local]Redback(config-if)#exit
[local]Redback(config-ctx)# interface fa-last-resort multibind lastresort
[local]Redback(config-if)#ip unnumbered loop1
[local]Redback(config-if)# exit

!Disable RADIUS authentication if services such as hotlining are not used:

[local]Redback(config-ctx)aaa authentication subscriber none
[local]Redback(config-ctx)exit

!Enable the local context and the mn-access interface for Mobile IP
services

[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mn-access
[local]Redback(config-mip-if)#exit

!Create the foreign agent, specify the CoA interface and create a home
```

```
agent peer

[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#care-of-address coa
[local]Redback(config-mip-fa)#home-agent-peer 172.16.2.1
[local]Redback(config-mip-hapeer)#end

! Configure the GE port for MN traffic and bind it to the MN access
interface

[local]Redback#config
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface mn-access local
[local]Redback(config-port)#exit

!Configure the IP-in-IP tunnel to the HA peer using the CoA as the local
endpoint
! Bind it to the HA peer interface in the local context

[local]Redback(config)#tunnel ipip HApeerTnl
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1
remote 172.16.2.1
[local]Redback(config-tunnel)#bind interface toHA-peer local
[local]Redback(config-tunnel)#end
```

3.2 Single FA Instance with Multiple HA Peers and IP-in-IP Tunnels

The following example creates an IP-in-IP tunnel and the interfaces to support an FA instance and two HA peers with overlapping IP addresses. The FA instance and tunnels are configured in the local context; each HA peer has its own VPN context. Traffic to and from the MNs is carried on the GE port **2/1:**

```
! Create the interfaces for the CoA and the MN access interface in the local
context

[local]Redback(config)#context local
[local]Redback(config-ctx)#interface coa loopback
[local]Redback(config-if)#ip address 20.1.1.1/16
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface mn-access
[local]Redback(config-if)#ip address 10.1.1.1/16
[local]Redback(config-if)# exit
[local]Redback(config-ctx)# interface loop1 loopback
[local]Redback(config-if)# ip address 192.168.1.1/32
[local]Redback(config-if)# exit
[local]Redback(config-ctx)# interface fa-last-resort multibind lastresort
[local]Redback(config-if)#ip unnumbered loop1
```

```
[local]Redback(config-if)# exit

!Disable RADIUS authentication if services such as hotlining are not used:

[local]Redback(config-ctx)aaa authentication subscriber none
[local]Redback(config-ctx)exit

! Create the contexts and tunnel interfaces for the HA peers (HoA-VPN  1
and HoA-VPN  2)

[local]Redback(config)#context hoa-vpn1

! Create the interface for the IP-in-IP tunnel endpoint for the HA
peer 1
[local]Redback(config-ctx)#interface toHApeer1

! Use the CoA IP address for the interface

[local]Redback(config-if)#ip 20.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)# interface loop1 loopback
[local]Redback(config-if)# ip address 192.168.1.1/32
[local]Redback(config-if)# exit
[local]Redback(config-ctx)# interface fa-last-resort multibind lastresort
[local]Redback(config-if)#ip unnumbered loop1
[local]Redback(config-if)# exit
[local]Redback(config)#context hoa-vpn2

! Create the interface for the IP-in-IP tunnel endpoint for the HA
peer 2

[local]Redback(config-ctx)#interface toHApeer2

! Use the CoA IP address for the interface

[local]Redback(config-if)#ip 20.1.1.1/24
[local]Redback(config-if)#exit
[local]Redback(config-ctx)# interface loop1 loopback
[local]Redback(config-if)# ip address 192.168.1.1/32
[local]Redback(config-if)# exit
[local]Redback(config-ctx)# interface fa-last-resort multibind
lastresort
[local]Redback(config-if)#ip unnumbered loop1
[local]Redback(config-if)# exit

! Enable the local context and the MN access interface for Mobile IP
visitors

[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mn-access
```

```
[local]Redback(config-mip-if)#exit

! Create the foreign agent and specify the care of interface

[local]Redback(config-mip)#foreign-agent
[local]Redback(config-mip-fa)#care-of-address coa

! Create the first home-agent peer and specify its context

[local]Redback(config-mip-fa)#home-agent-peer 172.16.2.1
[local]Redback(config-mip-hapeer)#vpn-context hoa-vpn1
[local]Redback(config-mip-hapeer)#exit

! Create the second home-agent peer and specify its context

[local]Redback(config-mip-fa)#home-agent-peer 172.16.2.2
[local]Redback(config-mip-hapeer)#vpn-context hoa-vpn2
[local]Redback(config-mip-hapeer)#end

! Configure the GE port for MN traffic and bind it to the MN access
interface

[local]Redback#config
[local]Redback(config)#port ethernet 2/1
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface mn-access local
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 2/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface toHApeer1 hoa-vpn1
[local]Redback(config-port)#exit

[local]Redback(config)#port ethernet 2/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface toHApeer2 hoa-vpn2
[local]Redback(config-port)#exit

! Configure the IP-in-IP tunnels to the HA peers
! Bind them to their interfaces in the HA peer VPN contexts
! Create the IP-in-IP tunnel to the HA-1 peer, using the CoA for the
local end

[local]Redback(config)#tunnel ipip HApeer1Tnl
[local]Redback(config-tunnel)#description IP-in-IP tunnel
circuit to HoA-VPN 1 peer
[local]Redback(config-tunnel)#peer-end-point local
20.1.1.1/24 remote 172.16.2.1 context local
[local]Redback(config-tunnel)#bind interface toHApeer1
hoa-vpn1
[local]Redback(config-tunnel)#no shutdown
[local]Redback(config-tunnel)#exit
```

```
! Create the IP-in-IP tunnel to the HA-2 peer; use the CoA for the
local end

[local]Redback(config)#tunnel ipip HApeer2Tnl
[local]Redback(config-tunnel)#description IP-in-IP tunnel
circuit to HoA-VPN 2 peer
[local]Redback(config-tunnel)#peer-end-point local
20.1.1.1/24 remote 172.16.2.2 context local
[local]Redback(config-tunnel)#bind interface toHApeer2
hoa-vpn2
[local]Redback(config-tunnel)#no shutdown
[local]Redback(config-tunnel)#exit
```

3.3 Configure a Link Aggregation Bundle as an FA Access Interface

The following example shows how to configure a link aggregation bundle as an FA access circuit and enable the interface for Mobile IP services:

```
! Create an 802.1Q-encapsulated access-link group

[local]Redback(config)#link-group foo access economical
[local]Redback(config-link-group)#encapsulation dot1q
[local]Redback(config-link-group)#dot1q pvc 100
[local]Redback(config-link-group)#bind interface mip-local
local

! Enable the local context and the MN access interface for Mobile IP
visitors

[local]Redback(config)#context local
[local]Redback(config-ctx)#router mobile-ip
[local]Redback(config-mip)#interface mip-local
[local]Redback(config-mip-if)#exit
```