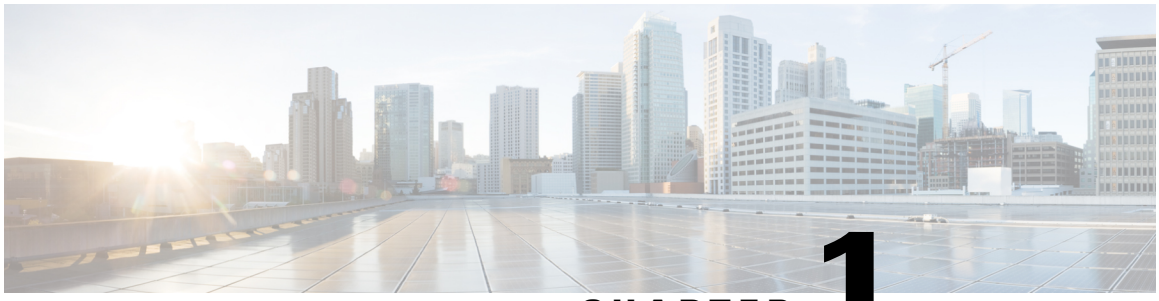
IP Mobility: Mobile IP Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring Mobile IP

This chapter describes how to configure Mobile IP. For a complete description of the Mobile IP commands in this chapter, refer to the "Mobile IP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* . To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Mobile IP Overview

If an IP node, for example, a personal digital assistant (PDA), moves from one link to another, the network prefix of its IP address no longer equals the network prefix assigned to its current link. As a result, packets are not delivered to the current location of the PDA.

Mobile IP enables an IP node to retain the same IP address and maintain existing communications while traveling from one link to another.

Mobile IP is an IETF standards based solution for mobility at the network layer, which is Layer 3. Mobile IP supports the following RFCs:

- RFC 2002, *IP Mobility Support*
- RFC 2003, *IP Encapsulation within IP*
- RFC 2005, *Applicability Statement for Mobile IP*
- RFC 2006, *The Definitions of Managed Objects for IP Mobility Support*

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

Why is Mobile IP Needed

New devices and business practices, such as PDAs and the next-generation of data-ready cellular phones and services, are driving interest in the ability of a user to roam while maintaining network connectivity. The requirement for data connectivity solutions for this group of users is very different than it is for the fixed dialup user or the stationary wired LAN user. Solutions need to accommodate the challenge of movement during a data session or conversation.

IP routing decisions are based on the network prefix of the IP address to be scalable for the Internet. All nodes on the same link share a common network prefix. If a node moves to another link, the network prefix does not equal the network prefix on the new link. Consequently, IP routing would fail to route the packets to the node after movement to the new link.

An alternative to network-prefix routing is host-specific routing. Host-specific routing is not a problem in small networks. However, considering there are billions of hosts on the Internet, this solution is not feasible for Internet connections. Routers would need enough memory to store tens of millions of routing table entries and would spend most of their computing resources updating routing tables.

DHCP (Dynamic Host Configuration Protocol) is commonly used in corporate environments and allows a server to dynamically assign IP addresses and deliver configuration parameters to nodes. The DHCP Server verifies the identity of the node, "leases" it the IP address from a pool of addresses for a predetermined period of time, and reclaims the address for reassignment when the lease expires. The node can terminate existing communication sessions, move to a new point-of-attachment to the network, reconnect to the network, and receive a new IP address from DHCP. This arrangement conserves IP addresses and reduces Internet access costs. However, if users are mobile and need continuous communications and accessibility without any interruptions in their sessions, DHCP is not an adequate solution. DHCP won't allow applications to maintain connections across subnet/network boundaries.

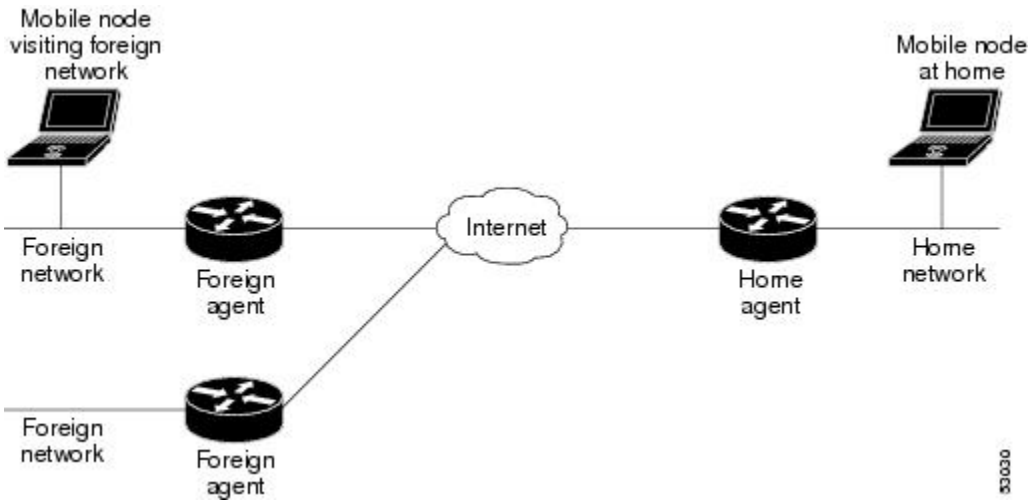
Mobile IP is scalable for the Internet because it is based on IP--any media that supports IP can support Mobile IP. Mobile IP does not drop the network prefix of the IP address of the node, which is critical to the proper routing of packets throughout the Internet. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses could compromise the network services. Certain applications, such as remote login, remote printing, and file transfers are examples of applications where it is undesirable to interrupt communications while a mobile node moves from one link to another. Thus, Mobile IP provides the solution for continuous connectivity that is scalable for the Internet.

Mobile IP Components

Mobile IP is comprised of the following three components, as shown in the figure below:

- Mobile node (MN)
- Home agent (HA)
- Foreign agent (FA)

Figure 1: Mobile IP Components and Relationships



An MN is a node, for example, a PDA, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This node can maintain ongoing communications while using only its home IP address.

An HA is a router on the home network of the MN that maintains an association between the home IP address of the MN and its *care-of address* , which is the current location of the MN on a foreign or visited network. The HA redirects packets by tunneling them to the MN while it is away from home.

An FA is a router on a foreign network that assists the MN in informing its HA of its current care-of address. The FA detunnels and delivers packets to the MN that were tunneled by the HA. The FA also acts as the default router for packets generated by the MN while it is connected to the foreign network.

It is recommended that HA and FA functionality be designed with interfaces with line protocol states that are normally up.

How Mobile IP Works

This section explains how Mobile IP works. The Mobile IP process includes three main phases, which are discussed in the following sections:

Agent Discovery

During the agent discovery phase, HAs and FAs advertise their presence on their attached links by periodically multicasting or broadcasting messages called *agent advertisements* . MNs listen to these advertisements and determine if they are connected to their home link or a foreign link. Rather than waiting for agent advertisements, an MN can also send an *agent solicitation.* This solicitation forces any agents on the link to immediately send an agent advertisement.

If an MN determines that it is connected to a foreign link, it acquires a care-of address. Two types of care-of addresses exist:

- FA care-of address
- Collocated care-of address

An FA care-of address is a temporary, loaned IP address that the MN acquires from the FA agent advertisement. This type of care-of address is the exit point of the tunnel from the HA to the FA. A collocated care-of address is an address temporarily assigned to an MN interface. This address is assigned by DHCP or by manual configuration.

Registration

After receiving a care-of address, the MN registers this address with its HA through an exchange of messages. The HA creates a *mobility binding table* that maps the home IP address of the MN to the current care-of address of the MN. An entry in this table is called a *mobility binding* . The main purpose of registration is to create, modify, or delete the mobility binding of an MN at its HA.

During registration, the MN also asks for service from the FA.

The HA advertises reachability to the home IP address of the MN, thereby attracting packets that are destined for that address. When a device on the Internet, called a *corresponding node* (CN), sends a packet to the MN, the packet is routed to the home network of the MN. The HA intercepts the packet and tunnels it to the registered care-of address of the MN. At the care-of address, the FA extracts the packet from the tunnel and delivers it to the MN.

If the MN is sending registration requests through a FA, the FA keeps track of all visiting MNs by keeping a visitor list. The FA relays the registration request directly to the HA without the need for tunneling. The FA serves as the router for all packets sent by the visiting MN.

When the MN powers down or determines that it is reconnected to its home link, it deregisters by sending a deregistration request to the HA. The HA then reclaims the MN.

Routing

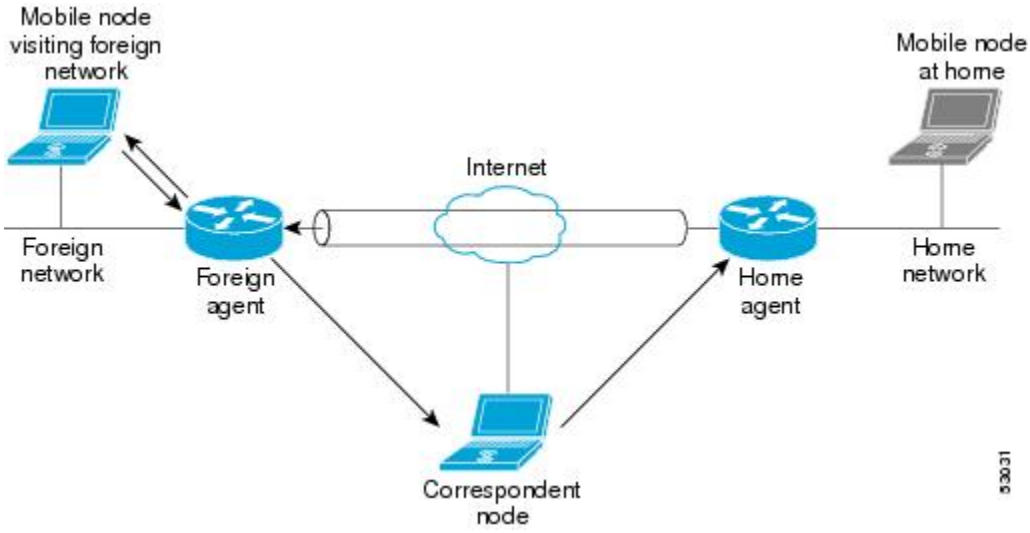
Because the major function of a Layer 3 protocol is routing, the major features of Mobile IP deal with how to route packets to users who are mobile.

Mobile IP is a tunneling-based solution that takes advantage of the Cisco-created generic routing encapsulation (GRE) tunneling technology and simpler IP-in-IP tunneling protocol. The traffic destined for the MN is forwarded in a triangular manner. When the CN (a device on the Internet) sends a packet to the MN, the HA redirects the packet by tunneling to the care-of address (current location) of the MN on the foreign network.

The FA receives the packet from the HA and forwards it locally to the MN. However, packets sent by the MN are routed directly to the CN.

See the figure below for a diagram of typical packet forwarding in Mobile IP.

Figure 2: Mobile IP Typical Packet Forwarding



Mobile IP Security

Mobile IP provides the following guidelines on security between its components:

- Communication between MN and HA must be authenticated.
- Communication between MN and FA can optionally be authenticated.
- Communication between FA and HA can optionally be authenticated.

Also, communication between an active HA and a standby HA, as implemented when using the HA redundancy feature, must be authenticated. For more information on this feature, see the Home Agent Redundancy, on page 7 section later in this chapter.

MN-HA

In particular, the Mobile IP registration process is vulnerable to security attacks, because it informs the HA where to tunnel packets to a traveling MN. An illegitimate node could send a bogus registration request to an HA and cause all packets to be tunneled to the illegitimate node instead of the MN. This type of attack, called a *denial-of-service attack* , prevents the MN from receiving and sending any packets. To prevent denial-of-service attacks, Mobile IP requires that all registration messages between an MN and an HA be authenticated.

Cisco IOS software supports the Mobile-Home Authentication Extension (MHAE). All registration messages between an MN and an HA include a mandatory authentication extension.

Message Digest 5 (MD5) is an algorithm that takes the registration message and a key to compute the smaller chunk of data, called a *message digest* , plus a secret key. The MN and HA both have a copy of the key, called a *symmetric key* , and authenticate each other by comparing the results of the computation.

The time stamp is an identifier in the message that ensures the origination of the registration request and the time it was sent, thereby preventing *replay attacks* . A replay attack occurs when an individual records an authentic message that was previously transmitted and replays it at a later time. The time stamp is also protected by MD5.

This authentication process begins when a MN sends the registration request. The MN adds the time stamp, computes the message digest, and appends the MHAE to the registration request. The HA receives the request, checks that the time stamp is valid, computes the message digest using the same key, and compares the message digest results. If the results match, the request is successfully authenticated. For the registration reply, the HA adds the time stamp, computes the message digest, and appends the MHAE to the registration reply. The MN authenticates the registration reply upon arrival from the HA.

MN-FA

Mobile IP does not require that communication between an MN and an FA be authenticated. Cisco IOS software supports the optional Mobile-Foreign Authentication Extension (MFAE). MFAE protects the communication between the MN and FA by keeping a shared key between them.

FA-HA

Mobile IP does not require that communication between an FA and an HA be authenticated. Cisco IOS software supports the optional Foreign-Home Authentication Extension (FHAE). FHAE protects the communication between the FA and HA by keeping a shared key between them.

HA-HA

Communication between an active HA and a standby HA in an HA redundancy topology must be authenticated. The authentication process works in the same manner as described in the previous MN-HA, on page 5 section. However, HA-HA authentication is an added Cisco-proprietary authentication extension needed to secure communication between peer HAs for HA redundancy. (Active HAs and standby HAs are peers to each other.)

Use the **ip mobile secure home-agent** global configuration command to configure the security associations between all peer HAs within a standby group for each of the other HAs within the standby group. The configuration is necessary because any HA within the standby group can become active HA or standby HA at any time. See the Mobile IP HA Redundancy Configuration Task List, on page 15 section later in this chapter for more information on HA-HA authentication.

Storing Security Associations

As discussed in the Mobile IP Security, on page 5 section earlier in this chapter, authentication between the MN and the HA involves keys. You can store the keys or *security associations* (SAs) on one of the following locations:

- NVRAM of an HA

- Authentication, authorization, and accounting (AAA) server that can be accessed using either TACACS+ or RADIUS

Because the NVRAM of an HA is typically limited, you should store the SAs on the HA only if your organization has a small number of MNs. If your organization has a large number of MNs, you should store the SAs on a AAA server.

Storing SAs on AAA

A AAA server can store a large number of SAs and scale well for future SA storage. It can accommodate not only the SAs for MN-HA authorization, but SAs for authorization between other Mobile IP components as well. Storing all SAs in a centralized location can streamline administrative and maintenance tasks related to the SAs.

Caching SAs on HA

When an MN is registering with an HA, keys are needed for the MN-HA authorization process, which requires AAA authorization for Mobile IP. If SAs are stored on a AAA server, the HA must retrieve the appropriate SA from the server. The SA is downloaded to the HA, and the HA caches the SA and reuses it when necessary rather than retrieving it from the AAA server again.

Home Agent Redundancy

During the Mobile IP registration process, an HA creates a mobility binding table that maps the home IP address of an MN to the current care-of address of the MN. If the HA fails, the mobility binding table will be lost and all MNs registered with the HA will lose their connectivity. To reduce the impact of an HA failure, Cisco IOS software supports the HA redundancy feature.

The functionality of HA redundancy runs on top of the Hot Standby Router Protocol (HSRP). HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic will immediately and transparently recover from failures.

HSRP Groups

Before configuring HA redundancy, you must understand the concept of HSRP groups.

An *HSRP group* is composed of two or more routers that share an IP address and a MAC (Layer 2) address and act as a single virtual router. For example, your Mobile IP topology can include one active HA and one or more standby HAs that the rest of the topology view as a single virtual HA.

You must define certain HSRP group attributes on the interfaces of the HAs so that Mobile IP can implement the redundancy. You can use the groups to provide redundancy for MNs with a home link on either the interface of the group (a *physical network*) or on virtual networks. *Virtual networks* are logical circuits that are programmed and share a common physical infrastructure.

How HA Redundancy Works

The HA redundancy feature enables you to configure an active HA and one or more standby HAs.

HA functionality is a service provided by the router and is not interface specific. Therefore, the HA and the MN must agree on which HA interface the MN should send its registration requests, and conversely, on which HA interface the HA should receive the registration requests. This agreement must factor in the following two scenarios:

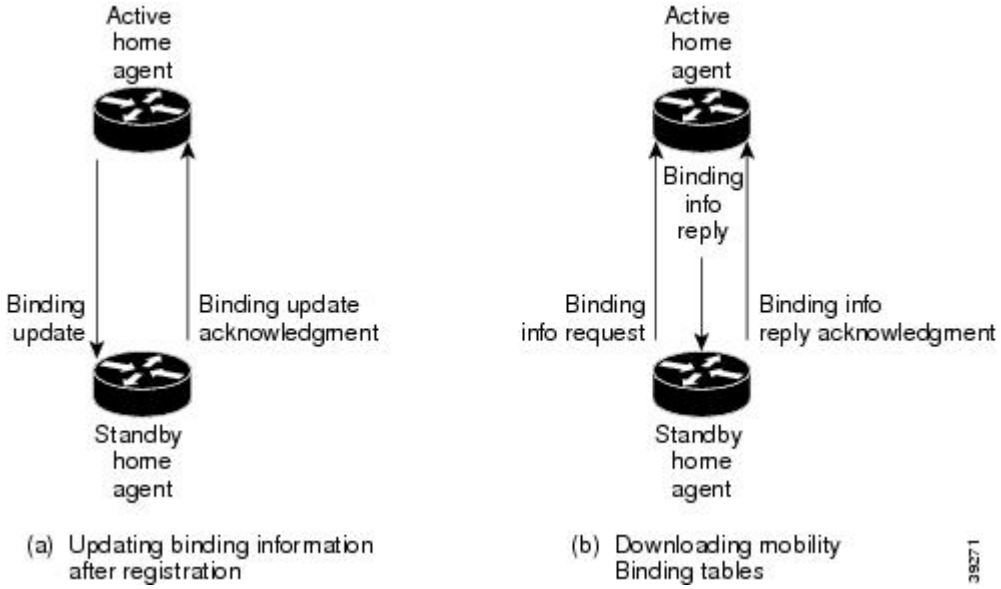
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN
- An MN that requires the HA interface to be on the same subnet as the MN, that is, the HA and the MN must be on the same home network

For MNs on physical networks, an active HA accepts registration requests from the MN and sends binding updates to the standby HA. This process keeps the mobility binding table on the active and standby HAs synchronized. See (a) in the figure below for an example of this process.

For MNs on virtual networks, the active and standby HAs are peers--either HA can handle registration requests from the MN and update the mobility binding table on the peer HA.

When a standby HA comes up, it must request all mobility binding information from the active HA. The active HA responds by downloading the mobility binding table to the standby HA. The standby HA acknowledges that it has received the requested binding information. See (b) in the figure below for an example of an active HA downloading the mobility bindings to a standby HA. A main concern in this stage of the process is which HA IP interface the standby HA should use to retrieve the appropriate mobility binding table and on which interface of the standby HA the binding request should be sent.

Figure 3: Mobility Binding Process



Managing Mobility Binding Tables

When a binding is cleared on an active home agent, it will not be cleared on the standby/peer home agent. If you want to clear the binding on the standby/peer home agent, you must manually clear it using the **clear ip mobile binding** command. This design ensures that binding information will not be accidentally lost.

It is possible that binding tables of two home agents in a redundancy group might be out of synchronization because of a network problem. You can force the synchronization of the binding tables by using the **clear ip mobile binding all load***standby-group-name* command.

Prerequisites

To configure home agent functionality on your router, you need to determine IP addresses or subnets for which you want to allow roaming service. If you intend to support roaming on virtual networks, you need to identify the subnets for which you will allow this service and place these virtual networks appropriately on the home agent. It is possible to enable home agent functionality for a physical or virtual subnet. In the case of virtual subnets, you must define the virtual networks on the router using the **ip mobile virtual-network** global configuration command. Mobile IP home agent and foreign agent services can be configured on the same router or on separate routers to enable Mobile IP service to users.

Because Mobile IP requires support on the host device, each mobile node must be appropriately configured for the desired Mobile IP service with client software. Please refer to the manual entries in your mobile aware IP stack vendor documentation for details.

Mobile IP Configuration Task List

To enable Mobile IP services on your network, you need to determine not only which home agents will facilitate the tunneling for selected IP address, but also where these devices or hosts will be allowed to roam. The areas, or subnets, into which the hosts will be allowed to roam will determine where foreign agent services need to be set up.

To configure Mobile IP, perform the tasks described in the following sections as related to the functions you intend to support. The tasks in the first two sections are required; the tasks in the remaining sections are optional.

Enabling Home Agent Services

Home agent functionality is useful within an enterprise network to allow users to retain an IP address while they move their laptop PCs from their desktops into conference rooms or labs or common areas. It is especially beneficial in environments where wireless LANs are used because the tunneling of datagrams hides the movement of the host and thus allows seamless transition between base stations. To support the mobility of users beyond the bounds of the enterprise network, home agent functionality can be enabled for virtual subnets on the DMZ or periphery of the network to communicate with external foreign agents.

To enable home agent service for users having homed or virtually homed IP addresses on the router, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **router mobile**
2. Router(config-router)# **exit**
3. Router(config)# **ip mobile home-agent**
4. Router(config)# **ip mobile virtual-network** *net mask*[**address** *address*]
5. Router(config)# **router** *protocol*
6. Router(config)# **redistribute mobile**
7. Router(config)# **ip mobile host** *lower* [*upper*] **virtual-network** *net mask*[**aaa** [**load-sa**]]
8. Router(config)# **ip mobile host** *lower*[*upper*] {**interface** *name*}
9. Router(config)# **ip mobile secure host** *lower-address*[*upper-address*]{**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*
10. Router(config)# **ip mobile secure foreign-agent** *address*{**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.
Step 3	Router(config)# **ip mobile home-agent**	Enables home agent service.
Step 4	Router(config)# **ip mobile virtual-network** *net mask*[**address** *address*]	Adds virtual network to routing table. If not using a virtual network, go to step 6.
Step 5	Router(config)# **router** *protocol*	Configures a routing protocol.
Step 6	Router(config)# **redistribute mobile**	Enables redistribution of a virtual network into routing protocols.
Step 7	Router(config)# **ip mobile host** *lower* [*upper*] **virtual-network** *net mask*[**aaa** [**load-sa**]]	Specifies mobile nodes (on a virtual network) and where their security associations are stored.[1]
Step 8	Router(config)# **ip mobile host** *lower*[*upper*] {**interface** *name*}	Specifies mobile nodes on an interface and where their security associations are stored. Omit this step if no mobile nodes are on the interface.
Step 9	Router(config)# **ip mobile secure host** *lower-address*[*upper-address*]{**inbound-spi** *spi-in* **outbound-spi** *spi-out*	**spi** *spi*} **key hex** *string*	Sets up mobile host security associations. Omit this step if using AAA.
Step 10	Router(config)# **ip mobile secure foreign-agent** *address*{**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*	(Optional) Sets up foreign agent security associations. Omit this step unless you have security associations with remote foreign agents.

1 By default, security associations are expected to be configured locally; however, the security association configuration can be offloaded to an AAA server.

Enabling Foreign Agent Services

Foreign agent services need to be enabled on a router attached to any subnet into which a mobile node may be roaming. Therefore, you need to configure foreign agent functionality on routers connected to conference room or lab subnets, for example. For administrators that want to utilize roaming between wireless LANs, foreign agent functionality would be configured on routers connected to each base station. In this case it is conceivable that both home agent and foreign agent functionality will be enabled on some of the routers connected to these wireless LANs.

To start a foreign agent providing default services, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **router mobile**
2. Router(config-router)# **exit**
3. Router(config)# **ip mobile foreign-agent care-of** *interface*
4. Router(config-if)# **ip mobile foreign-service**
5. Router(config)# **ip mobile secure home-agent** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*
6. Router(config)# **ip mobile secure visitor** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.
Step 3	Router(config)# **ip mobile foreign-agent care-of** *interface*	Sets up care-of addresses advertised to all foreign agent-enabled interfaces.
Step 4	Router(config-if)# **ip mobile foreign-service**	Enables foreign agent service on the interface.
Step 5	Router(config)# **ip mobile secure home-agent** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*	(Optional) Sets up home agent security association. Omit steps 4 and 5 unless you have security association with remote home agents or visitors.
Step 6	Router(config)# **ip mobile secure visitor** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out*	**spi** *spi*} **key hex** *string* [**replay timestamp**]	(Optional) Sets up visitor security association.

Configuring AAA in the Mobile IP Environment

To configure AAA in the Mobile IP environment, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa authorization ipmobile**{**tacacs+**| **radius**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **aaa new-model**	Enables the AAA access control model.
Step 2	Router(config)# **aaa authorization ipmobile**{**tacacs+**| **radius**}	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.

Configuring RADIUS in the Mobile IP Environment

Remote Authentication Dial-in User Service (RADIUS) is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information. For detailed information about RADIUS configuration options, refer to the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide* .

To configure RADIUS in the Mobile IP environment, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **radius-server host**
2. Router(config)# **radius-server key**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **radius-server host**	Specifies a RADIUS server host.
Step 2	Router(config)# **radius-server key**	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Configuring TACACS+ in the Mobile IP Environment

Terminal Access Controller Access Control System Plus (TACACS+) is an authentication protocol that provides remote access authentication and related services, such as event logging. For detailed information

about TACACS+ configuration options, refer to the "Configuring TACACS+" chapter in the *Cisco IOS Security Configuration Guide* .

To configure TACACS+ in the Mobile IP environment, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **tacacs-server host**
2. Router(config)# **tacacs-server key**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **tacacs-server host**	Specifies a TACACS+ server host.
Step 2	Router(config)# **tacacs-server key**	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

Verifying Setup

To make sure Mobile IP is set up correctly, use the following commands in EXEC mode as needed:

Command	Purpose
`Router#` **show ip mobile globals**	Displays home agent and foreign agent global settings.
`Router#` **show ip mobile host group**	Displays mobile node groups.
`Router#` **show ip mobile secure** {**host** | **visitor** | **foreign-agent** | **home-agent** | **summary**} *address*	Displays security associations.
`Router#` **show ip mobile interface**	Displays advertisements on interfaces.

Monitoring and Maintaining Mobile IP

To monitor and maintain Mobile IP, use any of the following EXEC commands:

Command	Purpose
`Router#` **show ip mobile host**	Displays mobile node counters (home agent only).
`Router#` **show ip mobile binding**	Displays mobility bindings (home agent only).
`Router#` **show ip mobile tunnel**	Displays active tunnels.
`Router#` **show ip mobile visitor**	Displays visitor bindings (foreign agent only).
`Router#` **show ip route mobile**	Displays Mobile IP routes.
`Router#` **show ip mobile traffic**	Displays protocol statistics.
`Router#` **clear ip mobile traffic**	Clears counters.
`Router#` **show ip mobile violation**	Displays information about security violations.
`Router#` **debug ip mobile advertise**	Displays advertisement information.[2]
`Router#` **debug ip mobile host**	Displays mobility events.

2 Make sure IRDP is running on the interface.

Shutting Down Mobile IP

To shut down Mobile IP, use the following commands in global configuration mode:

SUMMARY STEPS

1. Router(config)# **no ip mobile home-agent**
2. Router(config)# **no ip mobile foreign-agent**
3. Router(config)# **no router mobile**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **no ip mobile home-agent**	Disables home agent services.
Step 2	Router(config)# **no ip mobile foreign-agent**	Disables foreign agent services.
Step 3	Router(config)# **no router mobile**	Disables Mobile IP process.

Mobile IP HA Redundancy Configuration Task List

Enabling Mobile IP

To enable Mobile IP on the router, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **router mobile**	Enables Mobile IP on the router.

Enabling HSRP

To enable HSRP on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router (config-if)#` **standby** `[`*group-number*`]` **ip** *ip-address*	Enables HSRP.

Configuring HSRP Group Attributes

To configure HSRP group attributes that affect how the local router participates in HSRP, use either of the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)#` **standby** [*group-number*] **priority** *priority* [**preempt delay** [**minimum** | **sync**] *delay*]] or `Router(config-if)#` **standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*	Sets the Hot Standby priority used in choosing the active router. By default, the router that comes up later becomes standby. When one router is designated as an active HA, the priority is set highest in the HSRP group and the preemption is set. Configure the **preempt delay sync** command so that all bindings will be downloaded to the router before it takes the active role. The router becomes active when all bindings are downloaded or when the timer expires, whichever comes first.

Enabling HA Redundancy for a Physical Network

To enable HA redundancy for a physical network, use following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router (config-if)# **standby**[*group-number*] **ip** *ip-address*
2. Router(config-if)# **standby name** *hsrp-group-name*
3. Router(config)# **ip mobile home-agent standby** *hsrp-group-name*
4. Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router (config-if)# **standby**[*group-number*] **ip** *ip-address*	Enables HSRP.
Step 2	Router(config-if)# **standby name** *hsrp-group-name*	Sets the name of the standby group.
Step 3	Router(config)# **ip mobile home-agent standby** *hsrp-group-name*	Configures the home agent for redundancy using the HSRP group name.
Step 4	Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a

	Command or Action	Purpose
		security association needs to be set up between all HAs in the standby group.

Enabling HA Redundancy for a Virtual Network Using One Physical Network

To enable HA redundancy for a virtual network and a physical network, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router (config-if)# **standby**[*group-number*] **ip** *ip-address*
2. Router(config-if)# **standby name** *hsrp-group-name*
3. Do one of the following:
   - Router(config)# **ip mobile home-agent address** *address*
   -
   - Router(config)# **ip mobile home-agent**
4. Router(config)# **ip mobile virtual-network** *net* mask[**address** *address*]
5. Router(config)# **ip mobile home-agent standby** *hsrp-group-name*[[**virtual-network**] **address** *address*]
6. Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router (config-if)# **standby**[*group-number*] **ip** *ip-address*	Enables HSRP.
Step 2	Router(config-if)# **standby name** *hsrp-group-name*	Sets the name of the standby group.
Step 3	Do one of the following: • Router(config)# **ip mobile home-agent address** *address* • • Router(config)# **ip mobile home-agent** **Example:**	Defines a global home agent address. In this configuration, the address is the HSRP group address. Enter this command if the mobile node and home agent are on different subnets. or Enables and controls home agent services to the router. Enter this command if the mobile node and home agent are on the same subnet.

	Command or Action	Purpose
Step 4	Router(config)# **ip mobile virtual-network** *net* mask[**address** *address*]	Defines the virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.
Step 5	Router(config)# **ip mobile home-agent standby** *hsrp-group-name*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group to support virtual networks.
Step 6	Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Enabling HA Redundancy for a Virtual Network Using Multiple Physical Networks

To enable HA redundancy for a virtual network using multiple physical networks, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **standby**[*group-number*] **ip** *ip-address*
2. Router(config-if)# **standby name** *hsrp-group-name1*
3. Router(config-if)# **standby name** *hsrp-group-name2*
4. Do one of the following:
   - Router(config)# **ip mobile home-agent address** *address*
   -
   - Router(config)# **ip mobile home-agent**
5. Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]
6. Router(config)# **ip mobile home-agent standby** *hsrp-group-name1*[[**virtual-network**] **address** *address*]
7. Router(config)# **ip mobile home-agent standby** *hsrp-group-name2*[[**virtual-network**] **address** *address*]
8. Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **standby**[*group-number*] **ip** *ip-address*	Enables HSRP.

	Command or Action	Purpose
Step 2	Router(config-if)# **standby name** *hsrp-group-name1*	Sets the name of the standby HSRP group 1.
Step 3	Router(config-if)# **standby name** *hsrp-group-name2*	Sets the name of the standby HSRP group 2.
Step 4	Do one of the following: • Router(config)# **ip mobile home-agent address** *address* • • Router(config)# **ip mobile home-agent** **Example:**	Defines the global home agent address for virtual networks. In this configuration, the address is the loopback interface address. Enter this command if the mobile node and home agent are on different subnets. or Enables and controls home agent services to the router. Enter this command if the mobile node and home agent are on the same subnet.
Step 5	Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]	Defines the virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.
Step 6	Router(config)# **ip mobile home-agent standby** *hsrp-group-name1*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group 1 to support virtual networks.
Step 7	Router(config)# **ip mobile home-agent standby** *hsrp-group-name2*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group 2 to support virtual networks.
Step 8	Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Enabling HA Redundancy for Multiple Virtual Networks Using One Physical Network

To enable HA redundancy for multiple virtual networks using one physical network, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **standby**[*group-number*] **ip** *ip-address*
2. Router(config-if)# **standby name** *hsrp-group-name*
3. Do one of the following:
   - Router(config)# **ip mobile home-agent address** *address*
   -
   - Router(config)# **ip mobile home-agent**
4. Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]
5. Router(config)# **ip mobile home-agent standby** *hsrp-group-name*[[**virtual-network**] **address** *address*]
6. Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **standby**[*group-number*] **ip** *ip-address*	Enables the HSRP.
Step 2	Router(config-if)# **standby name** *hsrp-group-name*	Sets the name of the standby group.
Step 3	Do one of the following: • Router(config)# **ip mobile home-agent address** *address* • • Router(config)# **ip mobile home-agent** **Example:**	Defines a global home agent address. In this configuration, the address is the HSRP group address. Enter this command if the mobile node and home agent are on different subnets. or Enables and controls home agent services to the router. Enter this command if the mobile node and home agent are on the same subnet.
Step 4	Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]	Defines the virtual networks. Repeat this step for each virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.
Step 5	Router(config)# **ip mobile home-agent standby** *hsrp-group-name*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group to support virtual networks.
Step 6	Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Enabling HA Redundancy for Multiple Virtual Networks Using Multiple Physical Networks

To enable HA redundancy for multiple virtual networks using multiple physical networks, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router (config-if)# **standby**[*group-number*] **ip** *ip-address*
2. Router(config-if)# **standby name** *hsrp-group-name1*
3. Router(config-if)# **standby name** *hsrp-group-name2*
4. Do one of the following:
   - Router(config)# **ip mobile home-agent address** *address*
   -
   - Router(config)# **ip mobile home-agent**
5. Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]
6. Router(config)# **ip mobile home-agent standby** *hsrp-group-name1*[[**virtual-network**] **address** *address*]
7. Router(config)# **ip mobile home-agent standby** *hsrp-group-name2*[[**virtual-network**] **address** *address*]
8. Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router (config-if)# **standby**[*group-number*] **ip** *ip-address*	Enables the HSRP.
Step 2	Router(config-if)# **standby name** *hsrp-group-name1*	Sets the name of the standby HSRP group 1.
Step 3	Router(config-if)# **standby name** *hsrp-group-name2*	Sets the name of the standby HSRP group 2.
Step 4	Do one of the following: • Router(config)# **ip mobile home-agent address** *address* • • Router(config)# **ip mobile home-agent**	Defines the global home agent address for virtual networks. In this configuration, the address is the loopback interface address. Enter this command if the mobile node and home agent are on different subnets. or Enables and controls home agent services to the router. Enter this command if the mobile node and home agent are on the same subnet.
Step 5	Router(config)# **ip mobile virtual-network** *net mask* [**address** *address*]	Defines the virtual networks. Repeat this step for each virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.

	Command or Action	Purpose
Step 6	Router(config)# **ip mobile home-agent standby** *hsrp-group-name1*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group 1 to support virtual networks.
Step 7	Router(config)# **ip mobile home-agent standby** *hsrp-group-name2*[[**virtual-network**] **address** *address*]	Configures the home agent for redundancy using the HSRP group 2 to support virtual networks.
Step 8	Router(config)# **ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address *address* argument is that of the standby HA. If configured on the standby HA, the IP address *address* argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Verifying HA Redundancy

To verify that the Mobile IP Home Agent Redundancy feature is configured correctly on the router, perform the following steps:

SUMMARY STEPS

1. Enter the **show ip mobile globals**EXECcommand.
2. Examine global information for mobile agents.
3. Enter the **show ip mobile binding** [**home-agent** *address* | **summary**] EXEC command.
4. Examine the mobility bindings associated with a home agent address.
5. Enter the **show standby** EXEC command.
6. Examine information associated with the HSRP group.

DETAILED STEPS

Step 1 Enter the **show ip mobile globals**EXECcommand.

Step 2 Examine global information for mobile agents.

Step 3 Enter the **show ip mobile binding** [**home-agent** *address* | **summary**] EXEC command.

Step 4 Examine the mobility bindings associated with a home agent address.

Step 5 Enter the **show standby** EXEC command.

Step 6 Examine information associated with the HSRP group.

Monitoring and Maintaining HA Redundancy

To monitor and maintain HA redundancy, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router#` **debug ip mobile standby**	Displays debug messages for Mobile IP redundancy activities.
`Router#` **show ip mobile globals**	Displays the global home address if configured. For each Mobile IP standby group, displays the home agent address supported.
`Router#` **show ip mobile binding [home-agent** *address* | **summary]**	Displays mobility bindings with specific home agent address.

Mobile IP Configuration Examples

Home Agent Configuration Example

In the following example, the home agent has five mobile hosts on interface Ethernet1 (network 11.0.0.0) and ten on virtual network 10.0.0.0. There are two mobile node groups. Each mobile host has one security association. The home agent has an access list to disable roaming capability by mobile host 11.0.0.5. The 11.0.0.0 group has a lifetime of 1 hour (3600 seconds). The 10.0.0.0 group cannot roam in areas where the network is 13.0.0.0.

```
router mobile
!
! Define which hosts are permitted to roam
ip mobile home-agent broadcast roam-access 1
!
! Define a virtual network
ip mobile virtual-network 10.0.0.0 255.0.0.0
!
! Define which hosts are on the virtual network, and the care-of access list
ip mobile host 10.0.0.1 10.0.0.10 virtual-network 10.0.0.0 255.0.0.0 care-of-access 2
!
! Define which hosts are on Ethernet 1, with lifetime of one hour
ip mobile host 11.0.0.1 11.0.0.5 interface Ethernet1 lifetime 3600
!
! The next ten lines specify security associations for mobile hosts
! on virtual network 10.0.0.0
!
ip mobile secure host 10.0.0.1 spi 100 key hex 12345678123456781234567812345678
ip mobile secure host 10.0.0.2 spi 200 key hex 87654321876543218765432187654321
ip mobile secure host 10.0.0.3 spi 300 key hex 31323334353637383930313233343536
ip mobile secure host 10.0.0.4 spi 100 key hex 45678332353637383930313233343536
ip mobile secure host 10.0.0.5 spi 200 key hex 33343536313233343536373839303132
ip mobile secure host 10.0.0.6 spi 300 key hex 73839303313233343536313233343536
ip mobile secure host 10.0.0.7 spi 100 key hex 83930313233343536313233343536373
ip mobile secure host 10.0.0.8 spi 200 key hex 43536373839313233330313233343536
ip mobile secure host 10.0.0.9 spi 300 key hex 23334353631323334353637383930313
ip mobile secure host 10.0.0.10 spi 100 key hex 63738393132333435330313233343536
```

```
!
! The next five lines specify security associations for mobile hosts
! on Ethernet1
!
ip mobile secure host 11.0.0.1 spi 100 key hex 7383930331323334353631323334353536
ip mobile secure host 11.0.0.2 spi 200 key hex 8393031323334353631323334353637 3
ip mobile secure host 11.0.0.3 spi 300 key hex 4353637383931323333031323334353536
ip mobile secure host 11.0.0.4 spi 100 key hex 2333435363132333435363738393031 3
ip mobile secure host 11.0.0.5 spi 200 key hex 6373839313233343533031323334353536
!
! Deny access for this host
access-list 1 deny   11.0.0.5
!
! Deny access to anyone on network 13.0.0.0 trying to register
access-list 2 deny   13.0.0.0
```

Home Agent Using AAA Server Example

In the following AAA server configuration, the home agent can use a AAA server for storing security associations. Mobile IP has been authorized using a RADIUS server to retrieve the security association information, which is used by the home agent to authenticate registrations. This format can be imported into a CiscoSecure server.

```
user = 20.0.0.1 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}
user = 20.0.0.2 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}
user = 20.0.0.3 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}
```

In the example above, the user is the mobile node's IP address. The syntax for the security association is **spi#** *num* **="** *string* **"**, where *string* is the rest of the **ip mobile secure** {**host** | **visitor** | **home-agent** | **foreign-agent**} **key hex** *string* command.

The following example shows how the home agent is configured to use the AAA server:

```
aaa new-model
aaa authorization ipmobile radius
!
ip mobile home-agent
ip mobile virtual-network 20.0.0.0 255.0.0.0
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 255.0.0.0 aaa load-sa
!
radius-server host 1.2.3.4
radius-server key cisco
```

Foreign Agent Configuration Example

In the following example, the foreign agent is providing service on Ethernet1 interface, advertising care-of address 68.0.0.31 and a lifetime of 1 hour:

```
interface Ethernet0
 ip address 68.0.0.31 255.0.0.0
interface Ethernet1
```

```
ip address 67.0.0.31 255.0.0.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip mobile foreign-service
 ip mobile registration-lifetime 3600
!
router mobile
!
ip mobile foreign-agent care-of Ethernet0
```

Mobile IP HA Redundancy Configuration Examples

The table below summarizes the Mobile IP HA redundancy configuration required to support mobile nodes on physical and virtual home networks. Refer to this table for clarification as you read the examples in this section.

Table 1: Mobile IP HA Redundancy Configuration Overview

Mobile Node Home Network	Physical Connections	Home Agent Address	Configuration
Mobile Nodes with Home Agents on Different Subnets			
Physical network	Single	HSRP group address	**ip mobile home-agent standby** *hsrp-group-name*
Virtual network	Single	**ip mobile home-agent address** *address* In this configuration, *address* is the HSRP group address.	**ip mobile home-agent standby** *hsrp-group-name* **virtual-network**
Virtual network	Multiple	**ip mobile home-agent address** *address* In this configuration, *address*is the loopback interface address.	**ip mobile home-agent standby** *hsrp-group-name1* **virtual-network** **ip mobile home-agent standby** *hsrp-group-name2* **virtual-network** Repeat this command for each HSRP group associated with the physical connection.
Multiple virtual networks	Single	**ip mobile home-agent address** *address* In this configuration, *address* is the HSRP group address.	**ip mobile home-agent standby** *hsrp-group-name* **virtual-network**

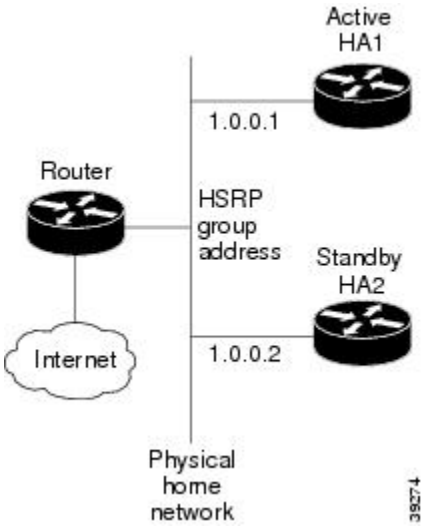
Mobile Node Home Network	Physical Connections	Home Agent Address	Configuration
Multiple virtual networks	Multiple	**ip mobile home-agent address** *address* In this configuration, *address*is the loopback interface address.	**ip mobile home-agent standby** *hsrp-group-name1* **virtual-network** **ip mobile home-agent standby** *hsrp-group-name2* **virtual-network** Repeat this command for each HSRP group associated with the physical connection.
Mobile Nodes with Home Agents on the Same Subnet			
Physical network	Single	HSRP group address	**ip mobile home-agent standby** *hsrp-group-name*
Virtual network	Single	**ip mobile virtual-network** *net mask* **address** *address* In this configuration, *address* is the loopback interface address.	**ip mobile home-agent standby** *hsrp-group-name* **virtual-network**
Virtual network	Multiple	**ip mobile virtual-network** *net mask* **address** *address* In this configuration, *address* is the loopback interface address.	**ip mobile home-agent standby** *hsrp-group-name1* **virtual-network** **ip mobile home-agent standby** *hsrp-group-name2* **virtual-network** Repeat this command for each HSRP group associated with the physical connection.
Multiple virtual networks	Single	**ip mobile virtual-network** *net mask* **address** *address* Repeat this command for each virtual network. The *address* argument is an address configured on the loopback interface to be on the same subnet. Specify the **ip address** *address mask* **secondary** interface configuration command to support multiple IP addresses configured on the same interface.	**ip mobile home-agent standby** *hsrp-group-name* **virtual-network**

Mobile Node Home Network	Physical Connections	Home Agent Address	Configuration
Multiple virtual networks	Multiple	**ip mobile virtual-network** *net mask* **address** *address* Repeat this command for each virtual network. The *address* argument is an address configured on the loopback interface to be on the same subnet. Specify the **ip address** *address mask* **secondary** interface configuration command to support multiple IP addresses configured on the same interface.	**ip mobile home-agent standby** *hsrp-group-name1* **virtual-network** **ip mobile home-agent standby** *hsrp-group-name2* **virtual-network** Repeat this command for each HSRP group associated with the physical connection.

HA Redundancy for Physical Networks Example

The figure below shows an example network topology for physical networks. The configuration example supports home agents that are on the same or a different physical network as the mobile node.

Figure 4: Topology Showing HA Redundancy on a Physical Network



HA1 is favored to provide home agent service for mobile nodes on physical network e0 because the priority is set to 110, which is above the default of 100. HA1 will preempt any active home agent when it comes up. During preemption, it does not become the active home agent until it retrieves the mobility binding table from the current active home agent or until 100 seconds expire for home agent synchronization.

Note If the **standby preempt** command is used, the preempt synchronization delay must be set or mobility bindings cannot be retrieved before the home agent preempts to become active.

The standby HSRP group name is SanJoseHA and the HSRP group address is 1.0.0.10. The standby HA uses this HSRP group address to retrieve mobility bindings for mobile nodes on the physical network. Mobile IP is configured to use the SanJoseHA standby group to provide home agent redundancy.

Mobile nodes are configured with HA address 1.0.0.10. When registrations come in, only the active home agent processes them. The active home agent sends a mobility binding update to the standby home agent, which also sets up a tunnel with the same source and destination endpoints. Updates and table retrievals are authenticated using the security associations configured on the home agent for its peer home agent. When packets destined for mobile nodes are received, either of the home agents tunnel them. If HA1 goes down, HA2 becomes active through HSRP and will process packets sent to home agent address 1.0.0.10.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110

 ip mobile home-agent standby SanJoseHA
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
 ip mobile home-agent standby SanJoseHA
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

HA Redundancy for a Virtual Network Using One Physical Network Example

This section presents two configuration examples:

- The mobile node and home agent are on different subnets.
- The mobile node and home agent are on the same subnet.

Mobile Node and Home Agent on Different Subnets

HA1 and HA2 share responsibility for providing home agent service for mobile nodes on virtual network 20.0.0.0. The home agents are connected on only one physical network.

The standby group name is SanJoseHA and the HSRP group address is 1.0.0.10. Mobile IP is configured to use the SanJoseHA standby group to provide home agent redundancy. Thus, HSRP allows the home agent to receive packets destined to 1.0.0.10.

This configuration differs from the physical network example in that a global HA address must be specified to support virtual networks. This address is returned in registration replies to the mobile node.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! specifies global HA address=HSRP group address to be used by all mobile nodes
 ip mobile home-agent address 1.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! specifies global HA address=HSRP group address to be used by all mobile nodes
 ip mobile home-agent address 1.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Mobile Node and Home Agent on Same Subnet

In this example, a loopback address is configured on the HA to be on the same subnet as the virtual network. A mobile node on a virtual network uses the HA IP address=loopback address configured for the virtual network. When a standby HA comes up, it uses this HA IP address to retrieve mobility bindings for mobile nodes on the virtual network.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! loopback to receive registration from MN on virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
ip mobile home-agent
! address used by Standby HA for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! loopback to receive registration from MN on virtual-network
 interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip mobile home-agent
```

```
! address used by Standby HA for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

HA Redundancy for a Virtual Network Using Multiple Physical Networks Example

This section presents two configuration examples:

- The mobile node and home agent are on different subnets.
- The mobile node and home agent are on the same subnet.

Mobile Node and Home Agent on Different Subnets

HA1 and HA2 share responsibility in providing home agent service for mobile nodes on virtual network 20.0.0.0. Both home agents are configured with a global home agent address of 10.0.0.10, which is the address of their loopback interface. This configuration allows home agents to receive registration requests and packets destined to 10.0.0.10.

The loopback address is used as the global HA address instead of the HSRP group addresses 1.0.0.10 and 2.0.0.10 to allow the HAs to continue serving the virtual network even if either physical network goes down.

Mobile nodes are configured with a home agent address 10.0.0.10. When registrations come in, either home agent processes them (depending on routing protocols) and updates the peer home agent. The home agent that receives the registration finds the first HSRP group that is mapped to 10.0.0.10 with a peer in the group and sends the update out that interface. If there is a network problem (for example, the home agent network adapter fails or cable disconnects), HSRP notices the absence of the peer. The home agent does not use that HSRP group and finds another HSRP group to use.

Note All routers must have identical loopback interface addresses, which will be used as the global HA address. However, do not use this address as the router ID for routing protocols.

When the peer home agent receives the registration update, both home agents tunnel the packets to the mobile nodes.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

interface ethernet1
 ip add 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

interface loopback0
 ip address 10.0.0.10 255.255.255.255

!Specifies global HA address=loopback address to be used by all mobile nodes
 ip mobile home-agent address 10.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
! Used to map to the HSRP group SanJoseHANet1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
! Used to map to the HSRP group SanJoseHANet2
```

```
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

interface ethernet1
 ip address 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

interface loopback0
 ip address 10.0.0.10 255.255.255.255

!Specifies global HA address=loopback address to be used by all mobile nodes
 ip mobile home-agent address 10.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
! Used to map to the HSRP group SanJoseHANet1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
! Used to map to the HSRP group SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Mobile Node and Home Agent on Same Subnet

In this example, a loopback address is configured on the HA to be on the same subnet as the virtual networks. A mobile node on a virtual network uses the HA IP address=loopback address configured for the virtual network. When a standby HA comes up, it uses this HA IP address to retrieve mobility bindings for mobile nodes on the virtual networks.

HA1 Configuration

```
interface ethernet0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1
interface ethernet1
 ip addr 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2
! loopback to receive registration from MN on virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip mobile home-agent
! address used by Standby HA for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
interface ethernet1
```

```
 ip address 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2
! loopback to receive registration from MN on virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip mobile home-agent
! address used by Standby HA for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

HA Redundancy for Multiple Virtual Networks Using One Physical Network Example

This section presents two configuration examples:

- The mobile node and home agent are on different subnets.
- The mobile node and home agent are on the same subnet.

The first figure below shows an example network topology for the first scenario. The second figure below shows an example network topology for the second scenario.

Figure 5: Topology Showing HA Redundancy on Multiple Virtual Networks Using One Physical Network (Different Subnets)

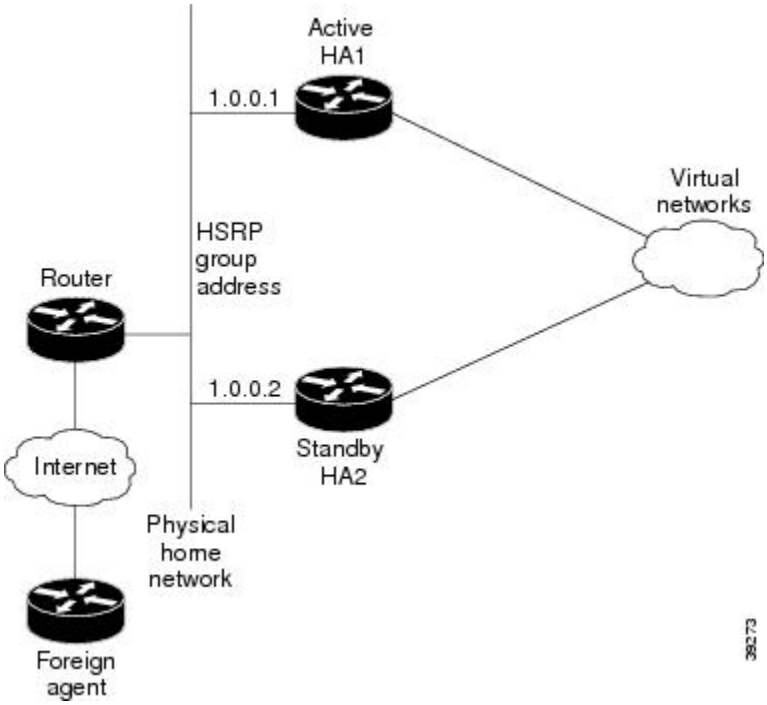
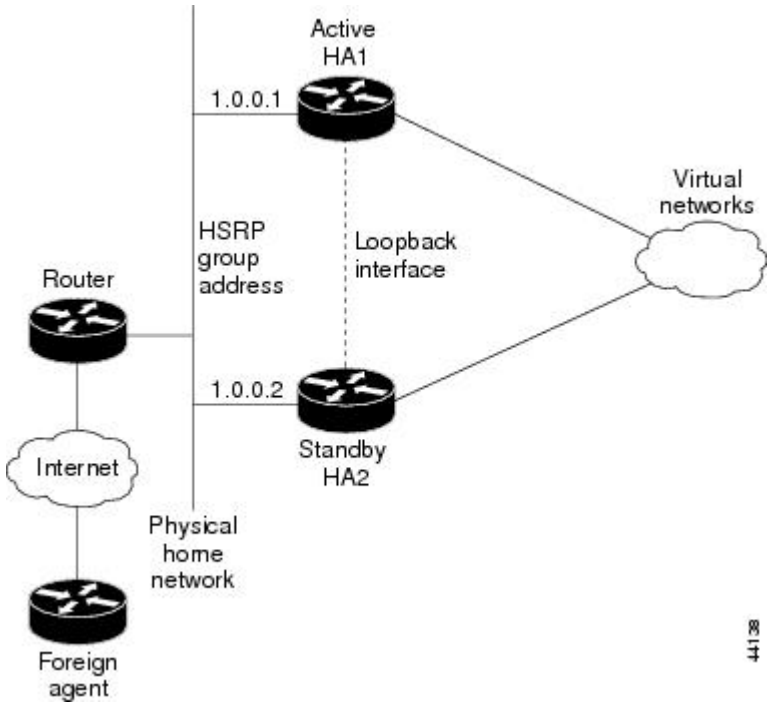


Figure 6: Topology Showing HA Redundancy on Multiple Virtual Networks Using One Physical Network (Same Subnet)



Mobile Node and Home Agent on Different Subnets

HA1 and HA2 share responsibility for providing home agent service for mobile nodes on virtual networks 20.0.0.0 and 30.0.0.0. The home agents are connected on only one physical network.

The standby group name is SanJoseHA and the HSRP group address is 1.0.0.10. Mobile IP is configured to use the SanJoseHA standby group to provide home agent redundancy. Thus, HSRP allows the home agent to receive packets destined to 1.0.0.10.

This configuration differs from the physical network example in that a global HA address must be specified to support virtual networks. This address is returned in registration replies to the mobile node.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! specifies global HA address=HSRP group address to be used by all mobile nodes
 ip mobile home-agent address 1.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
 ip mobile virtual-network 30.0.0.0 255.0.0.0
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! specifies global HA address=HSRP group address to be used by all mobile nodes
```

```
 ip mobile home-agent address 1.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
 ip mobile virtual-network 30.0.0.0 255.0.0.0
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Mobile Node and Home Agent on Same Subnet

For each virtual network, a loopback address is configured on the HA to be on the same subnet as the virtual network. It is only necessary to configure one loopback interface and to assign different IP addresses to the loopback interface for each virtual network using the **ip address** *ip-address mask* [**secondary**] interface configuration command. A mobile node on a particular virtual network uses the HA IP address =loopback address configured for that virtual network. When a standby HA comes up, it also uses this HA IP address to retrieve mobility bindings for mobile nodes on a particular virtual network.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! loopback to receive registration from MN on each virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip address 30.0.0.1 255.255.255.255 secondary
 ip mobile home-agent
! address used by Standby HA for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface e0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
! loopback to receive registration from MN on each virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip address 30.0.0.1 255.255.255.255 secondary
ip mobile home-agent
! address used by Standby HA for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

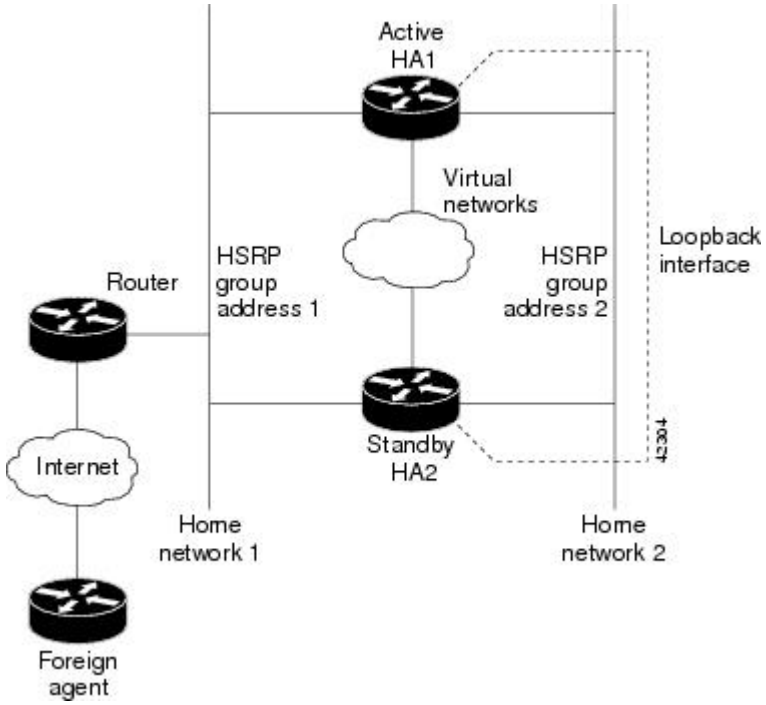
HA Redundancy for Multiple Virtual Networks Using Multiple Physical Networks Example

This section presents two configuration examples:

- The mobile node and home agent are on different subnets.
- The mobile node and home agent are on the same subnet.

The figure below shows an example network topology for this configuration type.

Figure 7: Topology Showing HA Redundancy on Virtual Networks Using Multiple Physical Networks



Mobile Node and Home Agent on Different Subnets

HA1 and HA2 share responsibility in providing home agent service for mobile nodes on virtual networks 20.0.0.0, 30.0.0.0, and 40.0.0.0. Both home agents are configured with a global home agent address of 10.0.0.10, which is the address of their loopback interface. This configuration allows home agents to receive registration requests and packets destined to 10.0.0.10.

The loopback address is used as the global HA address instead of the HSRP group addresses 1.0.0.10 and 2.0.0.10 to allow the HAs to continue serving the virtual networks even if either physical network goes down.

Mobile nodes are configured with home agent address 10.0.0.10. When registrations come in, either home agent processes them (depending on routing protocols) and updates the peer home agent. The home agent that receives the registration finds the first HSRP group that is mapped to 10.0.0.10 with a peer in the group and sends the update out that interface. If there is a network problem (for example, the home agent network adapter fails or cable disconnects), HSRP notices the absence of the peer. The home agent does not use that HSRP group and finds another HSRP group to use.

Note All routers must have identical loopback interface addresses, which will be used as the global HA address. However, do not use this address as the router ID for routing protocols.

When the peer home agent receives the registration update, both home agents tunnel the packets to the mobile nodes.

HA1 Configuration

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

interface ethernet1
 ip address 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2
interface loopback0
 ip address 10.0.0.10 255.255.255.255

!Specifies global HA address=loopback address to be used by all mobile nodes
 ip mobile home-agent address 10.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
 ip mobile virtual-network 30.0.0.0 255.0.0.0
 ip mobile virtual-network 40.0.0.0 255.0.0.0
! Used to map to the HSRP group SanJoseHANet1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
! Used to map to the HSRP group SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

interface ethernet1
 ip address 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

interface loopback0
 ip address 10.0.0.10 255.255.255.255

!Specifies global HA address=loopback address to be used by all mobile nodes
 ip mobile home-agent address 10.0.0.10
 ip mobile virtual-network 20.0.0.0 255.0.0.0
 ip mobile virtual-network 30.0.0.0 255.0.0.0
 ip mobile virtual-network 40.0.0.0 255.0.0.0
! Used to map to the HSRP group SanJoseHANet1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
! Used to map to the HSRP group SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Mobile Node and Home Agent on Same Subnet

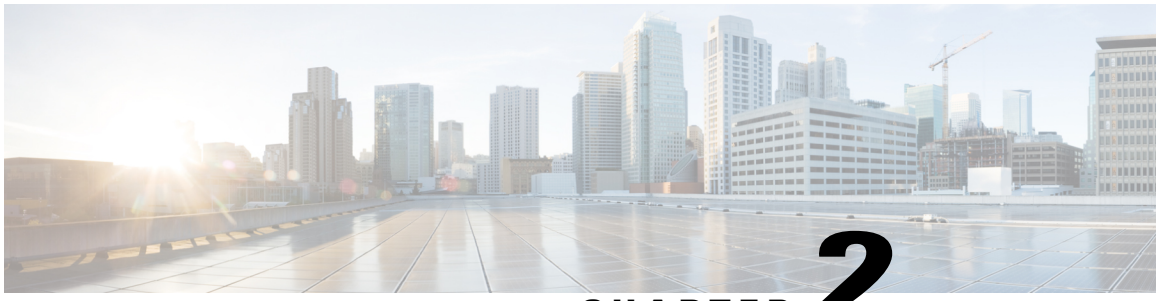
For each virtual network, a loopback address is configured on the HA to be on the same subnet as the virtual network. It is only necessary to configure one loopback interface and assign different IP addresses to the loopback interface for each virtual network, that is, using the **ip address** *ip-address mask* [**secondary**] interface configuration command. A mobile node on a particular virtual network uses the HA IP address =loopback address configured for that virtual network. When a standby HA comes up, it also uses this HA IP address to retrieve mobility bindings for mobile nodes on a particular virtual network.

HA1 Configuration

```
interface e0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1
interface ethernet1
 ip address 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2
! loopback to receive registration from MN on each virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip address 30.0.0.1 255.255.255.255 secondary
 ip address 40.0.0.1 255.255.255.255 secondary
ip mobile home-agent
! address used by Standby HA for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
 ip mobile virtual-network 40.0.0.0 255.0.0.0 address 40.0.0.1
! used to map to the HSRP groups SanJoseHANet1 and SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

HA2 Configuration

```
interface ethernet0
 ip address 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
interface ethernet1
 ip address 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2
! loopback to receive registration from MN on each virtual-network
interface loopback0
 ip address 20.0.0.1 255.255.255.255
 ip address 30.0.0.1 255.255.255.255 secondary
 ip address 40.0.0.1 255.255.255.255 secondary
ip mobile home-agent
! address used by Standby HA for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
 ip mobile virtual-network 40.0.0.0 255.0.0.0 address 40.0.0.1
! used to map to the HSRP groups SanJoseHANet1 and SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```



CHAPTER 2

Mobile IP MIB Support for SNMP

This document describes the Mobile IP MIB Support for SNMP feature in Cisco IOS Release 12.2(2)T. It includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

The Mobile IP MIB Support for SNMP feature adds a MIB module that expands network monitoring and management capabilities of foreign agent (FA) and home agent (HA) Mobile IP entities. Mobile IP management

using Simple Network Management Protocol (SNMP) is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB.

The RFC2006-MIB is a MIB module that uses the definitions defined in RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*. Beginning in Cisco IOS Release 12.2(1)T, RFC 2006 Set operations and an SNMP notification (trap) are supported. Set operations, performed from a network management system (NMS), allow you to use the RFC2006-MIB objects for starting and stopping the Mobile IP service, modifying and deleting security associations, modifying advertisement parameters, and configuring 'care-of addresses' for FAs. An SNMP notification for security violations can also be enabled on supported routing devices using the Cisco IOS software (see the Configuration Tasks, on page 43 section for details).

The CISCO-MOBILE-IP-MIB is a Cisco enterprise-specific extension to the RFC2006-MIB. The CISCO-MOBILE-IP-MIB allows you to monitor the total number of HA mobility bindings and the total number of FA visitor bindings using an NMS. These bindings are defined in the CISCO-MOBILE-IP-MIB as *cmiHaRegTotalMobilityBindings* and *cmiFaRegTotalVisitors* , respectively.

Benefits

The RFC2006-MIB defines a notification for Mobile IP entities (HA or FA) that can be sent to an NMS if there is a security violation. This notification can be used to identify the source of intrusions.

The RFC2006-MIB also defines a table (mipSecViolationTable) to log the security violations in the Mobile IP entities. This log can be retrieved from an NMS (using Get operations) and can be used to analyze the security violation instances in the system.

The CISCO-MOBILE-IP-MIB allows you to monitor the total number of HA mobility bindings. Customers can now obtain a snapshot of the current load in their HAs, which is important for gauging load at any time in the network and tracking usage for capacity planning.

Restrictions

The following restrictions exist for using Set operations on the following objects and tables in the RFC2006 MIB:

- mipEnable object--This object can be used to start and stop the Mobile IP service on the router. There are no issues with the Set support for this object.
- faRegistrationRequired object--This object controls whether the mobile node (MN) should register with the FA. The Cisco implementation of Mobile IP allows configuring this parameter at an interface level through the command line interface. However, this object is not defined at the interface level in the MIB. Therefore, Set support is not enabled for this object.
- mipSecAssocTable--This table allows the configuration of security associations between different Mobile IP entities (HA, FA, and MN). The index objects for this table are the IP address of the entity and security parameter index (SPI). To create a security association, the Cisco IOS software needs to know the correspondence between the IP address of the entity (used as index) and the kind of entity (FA, HA, or MN). No object in this table provides this information. Therefore, creation of rows in this table is not supported. The Cisco implementation allows only the modification of existing security associations. The table below shows the fixed values for objects in the mipSecAssocTable.

Table 2: Fixed Security Method for RFC2006-MIB mipSecAssocTable Objects

Object	Fixed Security Method Value
mipSecAlgorithmType	MD5
mipSecAlgorithmMod	prefixSuffix
mipSecReplayMethod	timestamps

When the mipSecKey object value is set with a Set operation, the value will be interpreted as an ASCII key if it contains printable ASCII values. Otherwise, the key will be interpreted as a hex string.

Because there is no rowStatus object in this table, deletion of rows in this table is achieved by setting the mipSecKey object to some special value. Existing security associations can be removed by setting the mipSecKey object to all zeros.

- maAdvConfigTable--This table allows modification of advertisement parameters of all advertisement interfaces in the mobility agent. Even though this table has a rowStatus object, row creation and destroy is not possible because creating a new row implies that an HA or FA service should be started on the interface corresponding to the new row. But no object in this table specifies the service (HA or FA) to be started. Therefore, there should already be one row corresponding to each interface on which the FA or HA service is enabled.

When the maAdvResponseSolicitationOnly object has a TRUE value, the maAdvMaxInterval, maAdvMinInterval, and maAdvMaxAdvLifetime objects of this table are not instantiated.

If the interface corresponding to a row is not up, the row will move to the notReady state.

- faCOATable--This table allows configuration of care-of addresses on an FA. This table has two objects: the rowStatus object and the index of the table. Row creation is not supported through createAndWait rowStatus because this table has only one object that can be set (rowStatus). The notInService state for rows in this table is not supported.

If the interface corresponding to the care-of address (configured by a row of this table) is not up, then the status of the row will be notReady. Creating a new row that corresponds to an interface that is not up is not possible.

Related Features and Technologies

- SNMP
- Mobile IP

Related Documents

This feature adds support for RFC 2006 Set operations and security violation traps. For specifications, see RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*.

For information on configuring SNMP using Cisco IOS software, refer to the following documents:

- The " Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2
- The " SNMP Commands" chapter of the *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.2

For information on using SNMP MIB features, refer to the appropriate documentation for your network management system.

For information on configuring Mobile IP using Cisco IOS software, refer to the following documents:

- The " Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide,* Release 12.2
- The " Mobile IP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2

Supported Platforms

Mobile IP support for SNMP functionality is available only in software images that support Mobile IP and SNMP. Supported platforms include the following:

- Catalyst 5000 family Route Switch Module (RSM)
- Catalyst 6000 family Multilayer Switch Feature Card (MSFC)
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000 series
- Cisco 7000 family (Cisco 7100 series, 7200 series, and 7500 series)
- Cisco uBR7200 series

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

- RFC2006-MIB
- CISCO-MOBILE-IP-MIB

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

RFCs

- RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*
- RFC 2002, *IP Mobility Support*

Prerequisites

The tasks in this document assume that you have configured SNMP and Mobile IP on your devices. Because this feature allows modification and deletion of security associations in the mipAssocTable through SNMP Set operations, use of SNMPv3 is strongly recommended.

Configuration Tasks

Configuring the Router to Send Mobile IP MIB Notifications

To configure the router to send Mobile IP traps or informs to a host, use the following commands in global configuration mode. Note that Mobile IP notifications need not be enabled on a system to process simple Set or Get SNMP requests.

Command	Purpose
`Router(config)#` **snmp-server enable traps ipmobile**	Enables the sending of Mobile IP notifications (traps and informs) for use with SNMP.
`Router(config)#` **snmp-server host** *host-addr* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] **ipmobile**	Specifies the recipient (host) for Mobile IP traps or informs.

Verifying Mobile IP MIB Configuration

Use the **more system:running-config** or the **show running-config** command to verify that the desired snmp-server commands are in your configuration file.

Monitoring and Maintaining Mobile IP MIBs

The Mobile IP MIB Support for SNMP feature is designed to provide information to network management applications (typically graphical-user-interface programs running on an external NMS). Mobile IP MIB objects can be read by the NMS using SNMP Set, Get, Get-next, and Get-bulk operations. Traps or informs can also be sent to the NMS by enabling the "ipmobile" notification type as described in the Configuration Tasks, on page 43 section.

Configuration Examples

In the following example, Mobile IP security violation notifications are sent to the host myhost.cisco.com as informs. The community string is defined as private1.

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 3 auth private1
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

New Command

- **snmp-server enable traps ipmobile**

Modified Command

- **snmp-server host**

Glossary

care-of address --An address used temporarily by a mobile node as a tunnel exit-point when the mobile node is connected to a foreign link.

foreign agent --A router on a visited network of a mobile node that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the home agent of the mobile node. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

home agent --A router on the home network of a mobile node that tunnels packets to the mobile node while it is away from home. It keeps current location information for registered mobile nodes called a mobility binding.

inform --An SNMP trap message that includes a delivery confirmation request. See "trap."

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a Network Management System (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

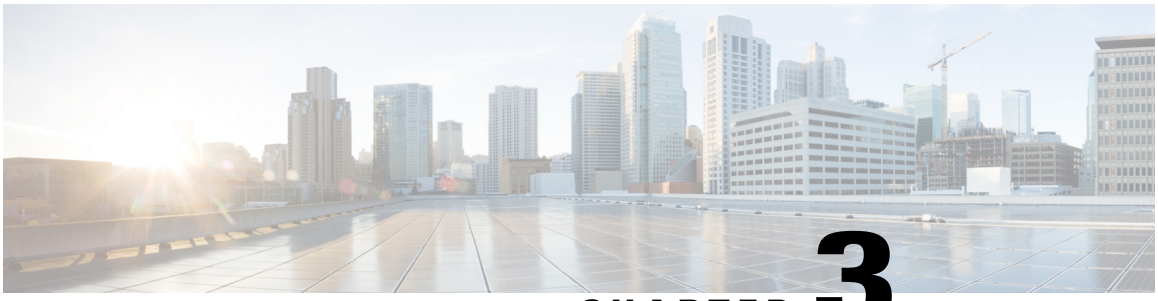
mobile node --A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming link-layer connectivity to a point of attachment is available.

NMS --network management system. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

SNMP --Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security, typically through the use of an NMS.

SPI --security parameter index. The index identifying a security context between a pair of nodes.

trap --Message sent by an SNMP agent to a network management station, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.



CHAPTER 3

Mobile IP NAT Detect

Network Address Translation (NAT) allows an organization with nonglobally routable addresses to connect to the Internet by translating those addresses into globally routable address space. Traditional Mobile IP tunneling has been incompatible with NAT. The Mobile IP--NAT Detect feature is a new service on the home agent that allows it to tunnel traffic to Mobile IP clients with private IP addresses behind a NAT-enabled device. The home agent is now capable of detecting a registration request that has traversed a NAT-enabled device and applying a tunnel to reach the Mobile IP client.

Feature Specifications for the Mobile IP: NAT Detect Feature

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
See Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Mobile IP NAT Detect

This feature is supported for mobile nodes using a collocated care-of address only. Mobile nodes using a foreign agent care-of address behind a NAT gateway cannot be detected by the home agent.

How to Configure Mobile IP NAT Detect

Configuring NAT Detect

To configure NAT detect on the home agent, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **exit**
5. **ip mobile home-agent** [**address** *ip-address*][**broadcast**] [**care-of-access** *access-list*] [**lifetime** *number*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *access-list*] [**suppress-unreachable**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 5	**ip mobile home-agent** [**address** *ip-address*][**broadcast**] [**care-of-access** *access-list*] [**lifetime** *number*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *access-list*] [**suppress-unreachable**] **Example:** `Router(config)# ip mobile home-agent nat-detect`	Enables home agent services and NAT detect.

Verifying the NAT Detect Configuration

To verify that the Mobile IP--NAT Detect feature is working, perform the following steps:

SUMMARY STEPS

1. **show ip mobile globals**
2. **show ip mobile binding**
3. **show ip mobile traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	Displays global information for mobile agents.

	Command or Action	Purpose
Step 2	**show ip mobile binding** **Example:** `Router# show ip mobile binding`	Displays the mobility binding table.
Step 3	**show ip mobile traffic** **Example:** `Router# show ip mobile traffic`	Displays protocol counters. • This command will show the number of successful registration requests using NAT detect.

Configuration Examples for Mobile IP NAT Detect

Home Agent with NAT Detect Example

In the following example, the home agent can detect registration requests from a mobile node behind a NAT-enabled router. The mobile node will use the NAT inside address as the collocated care-of address used in its registration requests.

Home Agent

```
ip routing
!
interface ethernet1
 ip address 1.0.0.1 255.0.0.0
!
interface ethernet2
 ip address 2.0.0.1 255.0.0.0
!
router mobile
!
router ospf 100
redistribute mobile subnets metric 1500
network 1.0.0.0 0.255.255.255 area 0
network 2.0.0.0 0.255.255.255 area 0
!
ip mobile home-agent lifetime 65535 nat-detect replay 255
ip mobile virtual-network 65.0.0.0 255.0.0.0
ip mobile host 65.1.1.1 65.1.1.10 virtual-network 65.0.0.0 255.0.0.0
ip mobile secure host 65.1.1.1 65.1.1.10 spi 100 key hex 12345678123456781234567812345678
!
```

Router Configured with NAT

```
ip routing
!
interface ethernet2
 ip address 2.0.0.2 255.0.0.0
 ip nat outside
```

```
!
interface e4
 ip address 4.0.0.1 255.0.0.0
 ip nat outside
!
! Outside address 2.0.0.101 used for any packet coming from inside 4.0.0.101
! 4.0.0.101 is the collocated care-of address used by MN to register
ip nat inside source static 4.0.0.101 2.0.0.101
router mobile
!
router ospf 100
network 2.0.0.0 0.255.255.255 area 0
network 4.0.0.0 0.255.255.255 area 0
!
```

Additional References

For additional information related to the Mobile IP--NAT Detect feature, refer to the following sections:

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the*Cisco IOS IP Configuration Guide,*Release 12.2.
Mobile IP commands	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* , Release 12.2
NAT configuration tasks	"Configuring IP Addressing" chapter in the *Cisco IOS IP Configuration Guide,*Release 12.2
NAT commands	"IP Addressing Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* , Release 12.2

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

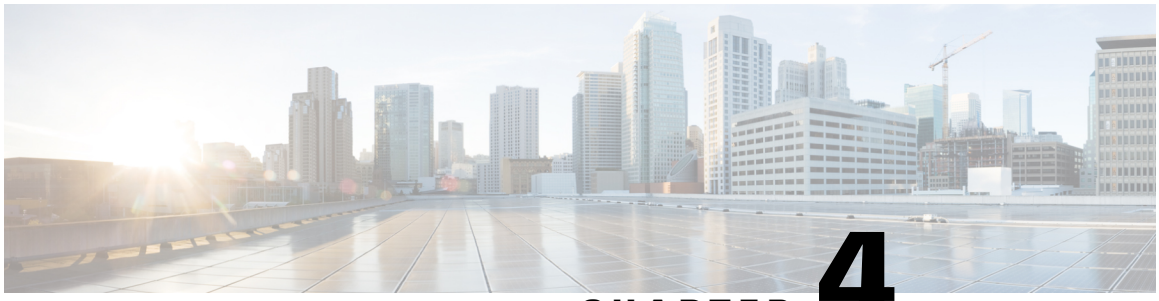
The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **ip mobile home-agent**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile traffic**

Glossary

care-of address --The termination point of the tunnel to a mobile node or mobile router. This can be a collocated care-of address, by which the mobile node or mobile router acquires a local address and detunnels its own packets, or a foreign agent care-of address, by which a foreign agent detunnels packets and forwards them to the mobile node or mobile router.

Note Refer to the Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 4

Mobile IP Support for Foreign Agent Reverse Tunneling

The Mobile IP--Support for Foreign Agent Reverse Tunneling feature prevents packets sent by a mobile node from being discarded by routers configured with ingress filtering by creating a reverse tunnel between the foreign agent and the home agent.

Feature Specifications for Mobile IP--Support for FA Reverse Tunneling

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Mobile IP Support for FA Reverse Tunneling

- Cisco Express Forwarding (CEF) switching is currently not supported on a foreign agent with reverse tunneling enabled. With CEF switching enabled, a foreign agent will not encapsulate the FA-HA tunnel header on traffic received from a mobile node or a mobile router. To disable CEF on the foreign agent, use the **no ip cef** global configuration command.

Foreign agent reverse tunneling may adversely impact process switching and fast switching performance when Mobile IP is enabled because:

- All packets arriving at the foreign agent from an interface that has reverse tunneling enabled need to be checked to determine if they need to be reverse tunneled.
- At the home agent only IP packets that contain a source address from an authenticated mobile user are decapsulated and allowed to enter a corporate network.

Before enabling foreign agent reverse tunneling, you should be aware of the following security considerations:

- It is possible for any mobile node to insert packets with the source address of a registered user. Enabling reverse tunneling on a foreign agent can increase this existing security consideration because reverse tunneling provides a one-way path into a private network. You can prevent this problem by enforcing link-layer authentication before permitting link-layer access.

See the part "Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2 *for more information, including instructions for configuring authentication.*

- If foreign agent reverse tunneling creates a tunnel that transverses a firewall, any mobile node that knows the addresses of the tunnel endpoints can insert packets into the tunnel from anywhere in the network. It is recommended to configure Internet Key Exchange (IKE) or IP Security (IPSec) to prevent this.

See the part "IP Security and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2 for more information, including instructions for configuring IKE and IPSec.

How to Enable Reverse Tunneling on a Foreign Agent

Enabling Foreign Agent Reverse Tunneling

The Cisco IOS implementation of foreign agent reverse tunneling is in the direct delivery style. In direct delivery, if the mobile node (a device such as a personal digital assistant that can change its point of attachment from one network to another) is using a foreign agent care-of address, it sends nonencapsulated packets to the foreign agent. The foreign agent detects the packets sent by the mobile node and encapsulates them before forwarding them to the home agent. If the mobile node is using a collocated care-of address, the foreign agent tunnels the unencapsulated packets directly to the home agent.

Perform this task to configure a foreign agent to provide default services, including reverse tunneling.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile foreign-agent care-of** *interface*
5. **ip mobile foreign-agent reverse-tunnel private-address**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip irdp**
9. **ip irdp maxadvertinterval** *seconds*
10. **ip irdp minadvertinterval** *seconds*
11. **ip irdp holdtime** *seconds*
12. **ip mobile foreign-service reverse-tunnel** [**mandatory**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**ip mobile foreign-agent care-of** *interface* **Example:** `Router(config)# ip mobile foreign-agent care-of serial0`	Enables foreign agent services when at least one care-of address is configured. • This is the foreign network termination point of the tunnel between the foreign agent and home agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.

	Command or Action	Purpose
Step 5	**ip mobile foreign-agent reverse-tunnel private-address** **Example:** `Router(config)# ip mobile foreign-agent reverse-tunnel private-address`	Forces a mobile node with a private home address to register with reverse tunneling.
Step 6	**interface** *type number* **Example:** `Router(config)# interface serial0`	Configures an interface and enters interface configuration mode.
Step 7	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.255.255`	Sets a primary IP address of the interface.
Step 8	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables ICMP Router Discovery Protocol (IRDP) processing on an interface.
Step 9	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 10`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 10	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 7`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 11	**ip irdp holdtime** *seconds* **Example:** `Router(config-if)# ip irdp holdtime 30`	(Optional) Length of time in seconds that advertisements are held valid. • Default is three times the **maxadvertinterval**period.
Step 12	**ip mobile foreign-service reverse-tunnel** [**mandatory**]	Enables foreign agent service on an interface. • Enables foreign agent reverse tunneling on the interface. This command also appends Mobile IP information such

	Command or Action	Purpose
	Example: `Router(config-if)# ip mobile foreign-service reverse-tunnel mandatory`	as care-of address, lifetime, and service flags to the advertisement.

Enabling Foreign Agent Reverse Tunneling on the Mobile Router

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile router**
5. **address** *address mask*
6. **home-agent** *ip-address*
7. **reverse-tunnel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.

	Command or Action	Purpose
Step 4	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the Mobile Router and enters mobile router configuration mode.
Step 5	**address** *address mask* **Example:** `Router(mobile-router)# address 10.1.0.1 255.255.255.255`	Sets the home IP address and network mask of the mobile router.
Step 6	**home-agent** *ip-address* **Example:** `Router(mobile-router)# home-agent 10.1.1.1`	Specifies the home agent that the mobile router uses during registration.
Step 7	**reverse-tunnel** **Example:** `Router(mobile-router)# reverse-tunnel`	Enables the reverse tunnel function.

Verifying Foreign Agent Service Configuration

Perform this task to optionally verify that the interface has been configured to provide foreign agent services, including foreign agent reverse tunneling.

SUMMARY STEPS

1. **enable**
2. **show ip mobile globals**
3. **show ip mobile interface**
4. **show ip mobile traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	(Optional) Displays global information for mobile agents.
Step 3	**show ip mobile interface** **Example:** `Router# show ip mobile interface`	(Optional) Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
Step 4	**show ip mobile traffic** **Example:** `Router# show ip mobile traffic`	(Optional) Displays protocol counters.

Additional References

The following sections provide additional references related to the Mobile IP--Support for FA Reverse Tunneling feature:

Related Documents

Related Topic	Document Title
Authentication	The part " Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2
IKE and IPSec security protocols	The part " IP ISecurity and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2
Mobile IP	Introduction to Mobile IP
Cisco mobile networks	Cisco Mobile Networks
Mobile wireless configuration	Cisco IOS Mobile Wireless Configuration Guide, Release 12.2
Mobile wireless commands	Cisco IOS Mobile Wireless Command Reference, Release 12.2

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs[3]	MIBs Link
• RFC2006-MIB • CISCO-MOBILE-IP-MIB	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

3 Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[4]	Title
RFC 2002	IP Mobility Support
RFC 2003	IP Encapsulation within IP
RFC 2005	Applicability Statement for IP Mobility Support
RFC 2006	The Definitions of Managed Objects for IP Mobility Support

RFCs[4]	Title
RFC 3024	*Reverse Tunneling for Mobile IP, revised*

4 Not all supported RFCs are listed.

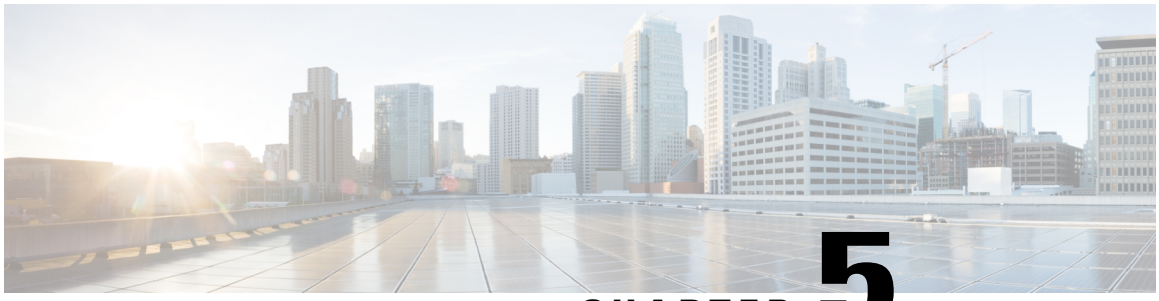
Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **debug ip mobile**
- **ip mobile foreign-agent**
- **ip mobile foreign-service**
- **show ip mobile traffic**



CHAPTER 5

Mobile IP Challenge and Response Extensions

The Mobile IP--Challenge/Response Extensions feature enables a foreign agent (FA) to authenticate a mobile node (MN) by sending mobile foreign challenge extensions (MFCE) and mobile node-AAA authentication extensions (MNAE) to the home agent (HA) in registration requests.

Feature Specifications for Mobile IP--Challenge/Response Extensions

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Mobile IP Challenge Response Extensions

In the Mobile IP--Challenge/Response Extensions feature, the foreign agent expects mobile node RRQs to contain the following extensions:

- Mobile node network address identifier
- MHAE
- Mobile node-foreign agent challenge extension
- Mobile node-AAA extension authenticator computed based on a shared secret between the mobile node and the AAA server.

If unique per-user passwords are configured on the AAA and the mobile nodes, and the mobile node or home agent security association is configured on the AAA server, the HA expects mobile node RRQs received from the FA CoA to contain the following:

- MFCE
- Mobile node -AAA extension authenticator

Restrictions for Mobile IP Challenge Response Extensions

The Mobile IP--Challenge/Response Extensions feature has the following restrictions:

- Mobile Node Colocated care-of address (CCOA) mode is not supported.

Information About Foreign Agent Challenge Response Extensions

Challenge Response Extensions

Mobile IP, as originally implemented, defines a Mobile-Foreign Authentication extension by which a mobile node can authenticate itself to a foreign agent. This Mobile-Foreign Authentication extension does not provide complete replay protection for the foreign agent and does not allow the foreign agent to use existing methods, such as Challenge Handshake Authentication Protocol (CHAP) to authenticate a mobile node. The Mobile IP--Foreign Agent Challenge/Response Extensions feature extends the Mobile IP agent advertisements and the registration requests that enable a foreign agent to use a challenge/response mechanism to authenticate a mobile node.

When the Mobile IP--Foreign Agent Challenge/Response Extensions feature is configured, the foreign agent expects the mobile node to include a challenge extension with a challenge value that the mobile node had previously advertised. The foreign agent also expects to receive this challenge extension within a specific time interval. The mobile node must also send an extension for authentication (MFAE or MN-AAA.)

How to Configure Foreign Agent Challenge Response Extensions

Configuring FA Challenge Response Extensions

Perform this task to configure a foreign agent to authenticate a mobile node by sending MFCEs and MNAEs in registration requests.

Before You Begin

If unique per-user passwords are configured on the AAA and the mobile nodes, and the mobile node or home agent security association is configured on the AAA server, the HA expects mobile node RRQs received from the FA CoA to contain the following:

- MFCE
- Mobile node -AAA extension authenticator

If the MFCE and MN-AAA extension authenticator are not forwarded to the home agent, the AAA server storing the mobile node/ home agent SAs must have identical passwords for all users to aid SA retrieval.

Note If the Mobile Node is registering in FA-COA mode and the Security Associations (SAs) must be obtained from AAA, the user password must be configured as "cisco".

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile foreign-agent care-of** *interface*
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip irdp**
8. **ip irdp holdtime** *seconds*
9. **ip irdp maxadvertinterval** *seconds*
10. **ip irdp minadvertinterval** *seconds*
11. **ip mobile foreign-service challenge** {**timeout** *value* | **window** *number*}
12. **ip mobile foreign-service challenge**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**ip mobile foreign-agent care-of** *interface* **Example:** `Router(config)# ip mobile foreign-agent care-of serial0`	Enables Foreign Agent services when at least one care-of address is configured. • This is the foreign network termination point of the tunnel between the Foreign Agent and Home Agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.
Step 5	**interface** *type number* **Example:** `Router(config)# interface serial0`	Configures an interface and enters interface configuration mode.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.255.255`	Sets a primary IP address of the interface.
Step 7	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables IRDP processing on an interface.
Step 8	**ip irdp holdtime** *seconds*	Length of time in seconds that advertisements are held valid.

	Command or Action	Purpose
	Example: `Router(config-if)# ip irdp holdtime 9000`	• Default is three times the **maxadvertinterval**period. When foreign agent challenge extensions are implemented, this value must be set to 9000 seconds.
Step 9	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 9000`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 10	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 7`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 11	**ip mobile foreign-service challenge** {**timeout** *value* | **window** *number*} **Example:** `Router(config-if)# ip mobile foreign-service challenge timeout 10`	Enables Foreign Agent service on an interface. • Configures the challenge timeout value and the number of valid recently sent challenge values.
Step 12	**ip mobile foreign-service challenge** **Example:** **forward-mfce** **Example:** `Router(config-if)# ip mobile foreign-service challenge forward-mfce`	Enables the foreign agent to send MFCEs to the home agent in registration requests.

Verifying Foreign Agent Service Configuration

Perform this task to optionally verify that the interface has been configured to provide foreign agent services.

SUMMARY STEPS

1. enable
2. show ip mobile globals
3. show ip mobile interface
4. show ip mobile traffic

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	(Optional) Displays global information for mobile agents.
Step 3	**show ip mobile interface** **Example:** `Router# show ip mobile interface`	(Optional) Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
Step 4	**show ip mobile traffic** **Example:** `Router# show ip mobile traffic`	(Optional) Displays protocol counters.

Additional References

The following sections provide additional references related to the Mobile IP--Challenge/Response Extensions feature:

Related Documents

Related Topic	Document Title
Authentication	The part " Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2

Related Topic	Document Title
IKE and IPSec security protocols	The part " IP Security and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2
Mobile IP	Introduction to Mobile IP
Cisco mobile networks	Cisco Mobile Networks
Mobile wireless configuration	Cisco IOS Mobile Wireless Configuration Guide, Release 12.2
Mobile wireless commands	Cisco IOS Mobile Wireless Command Reference, Release 12.2

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs[5]	MIBs Link
• RFC2006-MIB • CISCO-MOBILE-IP-MIB	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

5 Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random

password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[6]	Title
RFC 2002	IP Mobility Support
RFC 2003	IP Encapsulation within IP
RFC 2005	Applicability Statement for IP Mobility Support
RFC 2006	The Definitions of Managed Objects for IP Mobility Support
RFC 3024	*Reverse Tunneling for Mobile IP, revised*

6 Not all supported RFCs are listed.

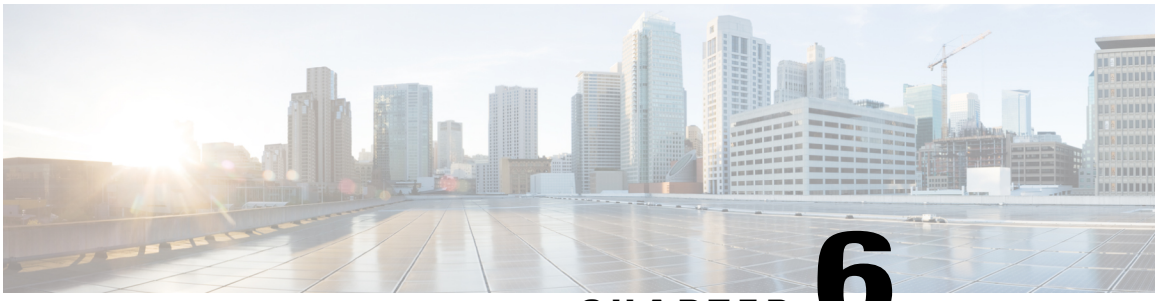
Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **debug ip mobile advertise**
- **ip mobile foreign-service**
- **show ip mobile traffic**



CHAPTER 6

Mobile IP Generic NAI Support and Home Address Allocation

The Mobile IP--Generic NAI Support and Home Address Allocation feature allows a mobile node to be identified by using a network access identifier (NAI) instead of an IP address (home address). The NAI is a character string that can be a unique identifier (username@realm) or a group identifier (realm). Additionally, this feature allows you to configure the home agent to allocate addresses to mobile nodes either statically or dynamically. Home address allocation can be from address pools configured locally on the home agent, through either Dynamic Host Configuration Protocol (DHCP) server access, or from the authentication, authorization, and accounting (AAA) server.

Feature Specifications for Mobile IP--Generic NAI Support and Home Address Allocation

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
Refer to Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Generic NAI Support and Home Address Allocation

NAI Overview

Authentication, Authorization, and Accounting (AAA) servers are used within the Internet to provide authentication and authorization services for dial-up computers. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either *user* or *user@realm* but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @realm portion, identifies a single user. The generic form allows all users in a given realm or without a realm to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server.

The original purpose of the NAI was to support roaming between dialup ISPs. With the NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each realm.

These services are also valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. The Mobile IP--Generic NAI Support and Home Address Allocation feature introduces a method for the mobile node to identify itself by including the NAI along with the Mobile IP registration request.

RFC 2794, *Mobile IP Network Access Identifier Extension for IPv4* , defines a mobile node NAI extension of type 131 to the Mobile IP registration messages. This extension must appear in the registration request before the mobile-home authentication extension (MHAE) and mobile-foreign authentication extension (MFAE). The home agent authenticates the mobile node and allocates an IP address. For static IP address allocation, the mobility binding is identified in the home agent as a flow {NAI, IP address} and for dynamic address assignment the mobility binding is identified by the NAI only.

Home Address Allocation

The home agent allocates a home address to the mobile node based on the NAI received during Mobile IP registration. The IP addresses can be statically or dynamically allocated to the mobile node. In addition, multiple static IP addresses can be allocated to the same NAI. The home agent will not permit simultaneous registrations for different NAIs with the same IP address, whether it is statically or dynamically allocated.

Static IP Addresses

Static IP addresses must be configured on the mobile node. The home agent supports static IP addresses that might be public IP addresses, or addresses in a private domain.

Note Use of private addresses for Mobile IP services requires reverse tunneling between the foreign agent and the home agent.

The mobile user proposes the configured/available address as a nonzero home address in the registration request message. The home agent can accept this address or return another address in the registration reply message. The home agent can authorize the IP address by accessing the AAA server or DHCP server. The AAA server may return the name of a local pool, or a single IP address. On successful Mobile IP registration, Mobile IP based services are made available to the user.

Local Authorization

A static address can be authorized on a per-mobile node or per-realm basis. Per-mobile node configurations require a specific NAI in the form of *user* or *user@realm* to be defined on the home agent and allow up to five addresses or a pool per NAI. Per-realm configurations require that a generic NAI be in the form of *@realm* and only allows address allocation from a local pool.

AAA Authorization

The number of mobile nodes that can be configured is limited because of NVRAM on the router. So, as an option, you can also store the authorized addresses or local pool name in a AAA server. Each user must have either the static-addr-pool attribute or the static-pool-def attribute configured in the AAA server. Unlike the static address configuration on the command line, the static-addr-pool attribute is not limited in the number of addresses. See the Configuration Examples for Generic NAI Support and Home Address Allocation, on page 85 section in this document for AAA configuration examples.

Static IP Address Configuration Priority

If the configuration exists locally as well as on the AAA server, the AAA configuration takes precedence over the local pool of addresses. The priority is given in the following order:

1. AAA addresses
2. AAA pool name
3. Local mobile node static addresses
4. Local pool

In cases where the static addresses list is retrieved from the AAA server but all the addresses are already in use by other mobile nodes, the next priority addressing mechanism is used.

Dynamic IP Addresses

A mobile node can request a dynamically allocated IP address by proposing an all-zero home address in the registration request message. The home agent allocates a home address and returns it to the mobile node in the registration reply message.

A fixed address is a dynamically assigned address that is always the same.

The home address can be allocated from a AAA server, a DHCP server, or configured locally through the command line interface (CLI). You can also define a local pool for address allocation on a AAA server or through the CLI.

DHCP

Optionally, Mobile IP uses the existing Cisco IOS DHCP proxy client to allocate dynamic home addresses by a DHCP server. The NAI is sent in the DHCP client-id option and can be used to provide dynamic DNS services.

AAA

Dynamic IP addressing from a AAA server allows support for fixed and or per session addressing for mobile nodes without the task of maintaining addressing at the mobile node or home agent. The AAA server can return either a specific address, a local pool name, or a DHCP server address.

Dynamic IP Address Configuration Priority

If the configuration exists locally as well as on the AAA server, the AAA configuration takes precedence over the local pool of addresses. The priority is given in the following order:

1. AAA address
2. AAA pool
3. Local mobile node address
4. Local pool

DHCP pool

Address Allocation for Same NAI with Multiple Static Addresses

The home agent supports multiple Mobile IP registrations for the same NAI with different static addresses through static address configuration on the command line or by configuring static-ip-address pool (s) at the AAA server or DHCP server. When the home agent receives a registration request message from the mobile user, the home agent accesses the AAA for authentication, and possibly for assignment of an IP address.

A single mobile user can use multiple static IP addresses either on the same IP device or multiple IP devices, while maintaining only one AAA record and security association. The ISP can then bill the user based on the NAI, independent of which IP device was used.

How Registrations Are Processed for the Same NAI

When the same NAI is used for registration from two different mobile IP devices, the behavior is as follows:

- If static address allocation is used in both cases, they are considered independent cases.
- If dynamic address allocation is used in both cases, the second registration replaces the first.
- If static is used for the first registration, and dynamic for the second, the dynamic address allocation replaces the static address allocation.
- If dynamic is used for the first registration, and static for the second, they are considered independent cases.

Additionally, two flows originating from the same mobile node using the same NAI, but two different home agents, are viewed as independent cases.

Benefits of Generic NAI Support and Home Address Allocation

- Provides a mechanism to identify users based on the NAI
- Supports static and dynamic IP address allocation
- Optimizes the use of IP addresses by reusing them

How to Configure Generic NAI Support and Home Address Allocation

Configuring the Home Agent

Perform one of the following tasks in this section, depending on whether you want to configure static IP addresses or dynamic IP addresses.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **ip local pool** {*named-address-pool*| **default**} {*first-ip-address*[*last-ip-address*]}
4. **ip mobile host** {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] } {**interface** *name* | **virtual-network** *network-address mask*} [**aaa** [**load-sa**]] [**care-of-access** *access-list*] [**lifetime** *number*]
5. **ip mobile secure host** {*lower*[*upper*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5**| **hmac-md5**} **mode prefix-suffix**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip local pool** {*named-address-pool*| **default**} {*first-ip-address*[*last-ip-address*]} **Example:** `Router(config)# ip local pool static-user-pool 172.21.58.3 172.21.58.254`	(Optional) Configures a local pool of IP addresses. • An NAI configured in the form of @realm can only be allocated addresses from a local pool.

Step 4	**ip mobile host** {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] } {**interface** *name* | **virtual-network** *network-address mask*} [**aaa** [**load-sa**]] [**care-of-access** *access-list*] [**lifetime** *number*]
	
	Example:
	`Router(config)# ip mobile host nai joe@staticuser.com local-pool static-user-pool interface FastEthernet0/0`
	
	Example:
	`Router(config)# ip mobile host nai joe static-address 172.21.58.3 172.21.58.4 interface FastEthernet0/0`
	
	Example:
	`Router(config)# ip mobile host nai joe@staticuser.com interface FastEthernet0/0 aaa`
		Configures the mobile host or mobile node group.
		• In the first example, a local pool named static-user-pool is used for static address allocation.
		• In the second example, multiple static addresses are configured and are associated with the same NAI. This configuration allows a single user to use multiple static IP addresses either on the same IP device or multiple IP devices, while maintaining only one AAA record and security association. Note that this option can only be used when the **nai** *string* is not a realm.
		• In the third example, the mobile host stores its authorized address in a AAA server. The appropriate attributes must be configured on the AAA server.

Step 5	**ip mobile secure host** {*lower*[*upper*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5**| **hmac-md5**} **mode prefix-suffix**] **Example:** `Router(config)# ip mobile secure host nai`	Specifies the mobility security associations for the mobile host. This step is optional only if you specify the **aaa** keyword in the **ip mobile host** command.

	Command or Action	Purpose
	`user@staticuser.com spi 100 key hex 12345678123456781234567812345678`	

Dynamic IP Addresses

This section describes how to configure the home agent to allocate dynamic IP addresses to mobile nodes.

Note

- The current implementation does not allow DHCP to be used with virtual networks.
- Local pool allocation cannot be used with the home agent redundancy feature.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **ip local pool** {*named-address-pool*| **default**} {*first-ip-address*[*last-ip-address*]}
4. **ip mobile host nai** string [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy-client**[**dhcp-server** *addr*]}] {**interface** *name*| **virtual-network** *network-address mask*} [**aaa** [**load-sa**]] [**care-of-access** *access-list*] [**lifetime** *number*]
5. **ip mobile secure host** {*lower*[*upper*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5**| **hmac-md5**} **mode prefix-suffix**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip local pool** {*named-address-pool*| **default**} {*first-ip-address*[*last-ip-address*]}	(Optional) Configures a local pool of IP addresses.

	Command or Action	Purpose
	Example: `Router(config)# ip local pool my-pool 172.21.58.5 172.21.58.250`	

Step 4	**ip mobile host nai** string [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy-client**[**dhcp-server** *addr*]}] {**interface** *name*| **virtual-network** *network-address mask*} [**aaa** [**load-sa**]] [**care-of-access** *access-list*] [**lifetime** *number*]
	Example:
	`Router(config)#ip mobile host nai jane@cisco.com address pool local my-pool interface FastEthernet0/0`
	Example:
	`Router(config)#ip mobile host nai jane@cisco.com address pool local my-pool virtual-network 10.2.0.0 255.255.0.0 aaa`
	Example:
	`Router(config)# ip mobile host nai jane@cisco.com address pool dhcp-proxy-client dhcp-server 10.1.2.3 interface FastEthernet 0/0`
		Configures the mobile host or mobile node group.
		• In the first example, a local pool named my-pool is used for dynamic address allocation.
		• In the second example, the user name is sent to the AAA server. If no address allocation information comes back from the AAA server, the home agent will assign an available address from the pool named my-pool.
		• In the third example, a DHCP proxy client specifies that a DHCP server, located at 10.1.2.3, will allocate dynamic home addresses.

Step 5	**ip mobile secure host** {*lower*[*upper*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5**| **hmac-md5**} **mode prefix-suffix**] **Example:** `Router(config)# ip mobile secure host nai jane@cisco.com spi 100 key hex 12345678123456781234567812345678`	Specifies the mobility security associations for the mobile host. Optional only if you specify the **aaa** keyword in the **ip mobile host** command.

Configuring AAA in the Mobile IP Environment

Access control is the way you manage who has user access to the network server and what services the users are allowed to use. AAA network security services provide the primary framework through which you set up access control on your router or access server. See the Configuration Examples for Generic NAI Support and Home Address Allocation, on page 85 in this document for example AAA configurations.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]
5. **aaa authorization ipmobile** {**tacacs+**| **radius**}
6. **aaa session-id** [**common**| **unique**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA access control.
Step 4	**aaa authentication login** {**default**	*list-name*} *method1* [*method2*...] **Example:** `Router(config)# aaa authentication login default enable`	Sets AAA authentication at login.
Step 5	**aaa authorization ipmobile** {**tacacs+**| **radius**} **Example:** `Router(config)# aaa authorization ipmobile radius`	Specifies which AAA protocol to be used by Mobile IP.
Step 6	**aaa session-id** [**common**| **unique**] **Example:** `Router(config)# aaa session-id common`	Ensures that the same session ID will be used for each AAA accounting service type within a call.

Configuring RADIUS in the Mobile IP Environment

Remote Authentication Dial-in User Service (RADIUS) is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **radius-server host** {**hostname** | ip-address}[**auth-port** *port-number*] [**acct-port** *port-number*]
4. **radius-server retransmit** *retries*
5. **radius-server key** {0 *string* |7 *string* | *string*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {**hostname**	ip-address}[**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 128.107.162.173 auth-port 1645 acct-port 1646`	Specifies a RADIUS server host.
Step 4	**radius-server retransmit** *retries* **Example:** `Router(config)# radius-server retransmit 3`	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.

	Command or Action	Purpose
Step 5	**radius-server key** {0 *string* |7 *string* | *string*} **Example:** `Router(config)# radius-server key cisco`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Verifying Generic NAI Support and Home Address Allocation

To verify generic NAI support and home address allocation, use the following commands in privileged EXEC mode, as needed:

SUMMARY STEPS

1. **show ip mobile binding nai** *string*
2. **show ip mobile host nai** *string*
3. **show ip mobile visitor nai** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip mobile binding nai** *string* **Example:** `Router# show ip mobile binding nai jane@cisco.com`	Displays the mobility binding table. • See the Output Examples, on page 84 section for an example.
Step 2	**show ip mobile host nai** *string* **Example:** `Router# show ip mobile host nai jane@cisco.com`	Displays mobile node information. • See the Output Examples, on page 84 section for an example.
Step 3	**show ip mobile visitor nai** *string* **Example:** `Router# show ip mobile visitor nai jane@cisco.com`	Displays the visitor list on the foreign agent. • See the Output Examples, on page 84 section for an example.

Output Examples

This section provides the following output examples:

Sample Output for the show ip mobile binding Command

In this example, output information about all current mobility bindings is displayed using the **show ip mobile binding**EXEC command:

```
Router> show ip mobile binding nai jane@cisco.com
Mobility Binding List:
jane@cisco.com (Bindings 1):
    Home Addr 25.2.2.1
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags Sbdmgvt, Identification B750FAC4.C28F56A8,
    Tunnel2 src 1.1.1.1.dest 2.2.2.1 reverse-allowed
    Routing Options - (B)Broadcast
```

Sample Output for the show ip mobile host Command

In this example, mobile host counters and information is displayed using the **show ip mobile host**EXEC command:

```
Router> show ip mobile host nai jane@cisco.com
jane@cisco.com:
    Dynamic address from local pool dynamic-pool
    Allowed lifetime 00:03:20 (200/default)
    Roaming status -registered-, Home link on virtual network 25.0.0.0/8
    Bindings 25.2.2.1
    Accepted 2, Last time 04/13/02 19:04:28
    Overall service time 00:04:42
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
```

Sample Output for the show ip mobile visitor Command

In this example, the visitor list on the foreign agent is displayed using the **show ip mobile visitor**EXEC command:

```
Router> show ip mobile visitor nai jane@cisco.com
Security Associations (algorithm,mode,replay)
Mobile Visitor List:
jane@cisco.com
    Home addr 25.2.2.2
    Interface Ethernet3/2, MAC addr 0060.837b.95ec
    IP src 0.0.0.0, dest 2.2.2.1, UDP src port 434
    HA addr 1.1.1.1, Identification B7510E60.64436B38
    Lifetime 00:03:20 (200) Remaining 00:02:57
    Tunnel2 src 2.2.2.1, dest 1.1.1.1, reverse-allowed
    Routing Options - (B) Broadcast
```

Configuration Examples for Generic NAI Support and Home Address Allocation

Static Home Addressing Using NAI Examples

The following example configures a local pool of static addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
router mobile
!
ip local pool mobilenodes 172.21.58.3 172.21.58.250
ip mobile host nai @cisco.com static-address local-pool mobilenodes
ip mobile secure host nai @cisco.com spi 100 key hex 12345678123456781234567812345678
!
```

Dynamic Home Addressing Using NAI Examples

The following is an example of dynamic addressing using a local pool:

```
router mobile
!
ip local pool my-pool 10.1.2.3 10.1.2.5
ip mobile host nai jane@cisco.com address pool local my-pool virtual-network 10.0.0.0
255.255.255.0
ip mobile secure host nai jane@cisco.com spi 100 key hex 12345678123456781234567812345678
```

The following is an example of dynamic addressing using a DHCP server specified by the DHCP proxy client:

```
router mobile
!
ip mobile host nai jane@cisco.com address pool dhcp-proxy-client dhcp-server 10.1.2.3
interface FastEthernet 0/0
ip mobile secure host nai jane@cisco.com spi 100 key hex 12345678123456781234567812345678
```

Home Agent Using NAI AAA Server Example

In the following static configuration, the home agent can use a AAA server to store either the authorized addresses or local pool name. For the mobile node to request a static address, either the static-addr-pool attribute or the static-pool-def attribute must be configured on the AAA server.

Home Agent

The following example shows how the home agent is configured to use the AAA server:

```
aaa new-model
aaa authorization ipmobile radius
!
ip local pool mobilenodes 10.0.0.5 10.0.0.10
ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

Radius Attributes

```
Cisco-AVPair = "mobileip:static-addr-pool=10.0.0.1 10.0.0.2 10.0.0.3"
Cisco-AVPair = "mobileip:static-pool-def=mobilenodes"
```

AAA and Local Configuration Example

You can also configure some addressing details on the home agent and some on the AAA server. In the following example, a set of authorized static addresses for a mobile node are configured on the AAA server and the dynamic addresses are configured locally on the home agent.

Home Agent

```
ip mobile host nai @cisco.com address pool local mobilenodes interface ethernet2/1 aaa
```

Radius Attribute

```
Cisco-AVPair = "mobileip:static-addr-pool=10.2.0.1 10.2.0.2 10.0.0.3"
```

Additional References

For additional information related to generic NAI support and home address assignment, refer to the following sections:

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the*Cisco IOS IP Configuration Guide,* Release 12.2
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2
AAA configuration tasks	*Cisco IOS Security Configuration Guide,* Release 12.2
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference,* Release 12.2

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs[7]	MIBs Link
• CISCO-MOBILE-IP MIB	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

7 Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[8]	Title
RFC 2486	*The Network Access Identifier*
RFC 2794	*Mobile IP Network Access Identifier Extension for IPv4*
RFC 3220	*IP Mobility Support for IPv4*

8 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **clear ip mobile binding**
- **clear ip mobile host-counters**
- **clear ip mobile secure**
- **clear ip mobile visitor**
- **ip mobile home-agent**
- **ip mobile home-agent reject-static-address**
- **ip mobile host**
- **ip mobile secure**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile host**
- **show ip mobile secure**
- **show ip mobile violation**
- **show ip mobile visitor**

Glossary

home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding.

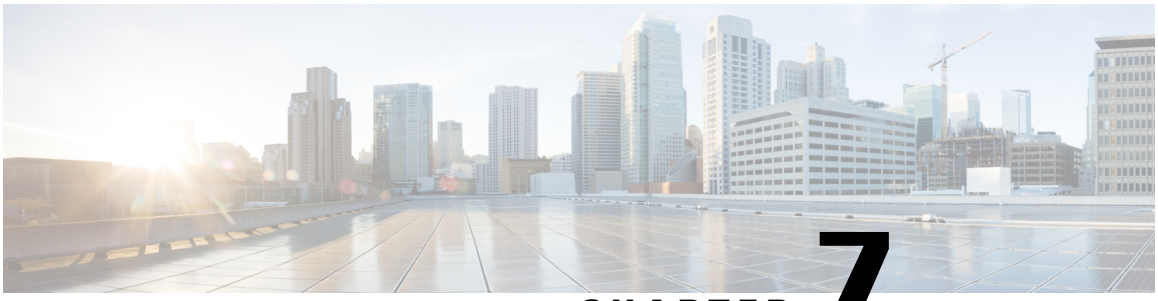
flow --In the context of this document, a flow is the set of {NAI, IP Address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on.

foreign agent --A router on the visited network of a foreign network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers packets to the mobile node or mobile router that were tunneled by the Home Agent of the mobile node. For packets sent by a mobile node, the Foreign Agent may serve as a default router for registered mobile nodes.

mobility binding --The association of a home address with a care-of address and the remaining lifetime.

NAI --Network Access Identifier. The user ID submitted by the mobile node during registration to identify the user for authentication. The NAI may help route the registration request to the right home agent.

Note Refer to the Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 7

Mobile IP Home Agent Policy Routing

The Mobile IP Home Agent Policy Routing feature supports route maps on Mobile IP tunnels created at the home agent. This feature allows an Internet Service Provider (ISP) to provide service to multiple customers. While reverse tunneling packets, the home agent looks up where the packet should go. For example, if an address corresponds to a configured network access identifier (NAI) realm name (such as cisco.com), the packet goes out interface 1, which has a connection to the Cisco network. If an address corresponds to another NAI realm name (such as company2.com), the packet goes out interface 2, which has a connection to the Company2 network.

Feature Specifications for Mobile IP Home Agent Policy Routing

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
Refer to Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Mobile IP Home Agent Policy Routing

Reverse tunnelling must be enabled on both the home agent and foreign agent.

Information About Mobile IP Home Agent Policy Routing

Policy Routing

Policy routing is a more flexible mechanism for routing packets than destination routing. Policy routing allows network administrators to implement policies that selectively cause packets to take different paths. The policy can be as simple as not allowing any traffic from a department on a network or as complex as making sure traffic with certain characteristics originating within a network takes path A, while other traffic takes path B.

Policy routing is applied to incoming packets. All packets received on an interface with policy routing enabled are considered for policy routing. The router passes the packets through enhanced packet filters called route maps. The route map determines which packets are routed to which router next. Based on the criteria defined in the route maps, packets are forwarded/routed to the appropriate next hop.

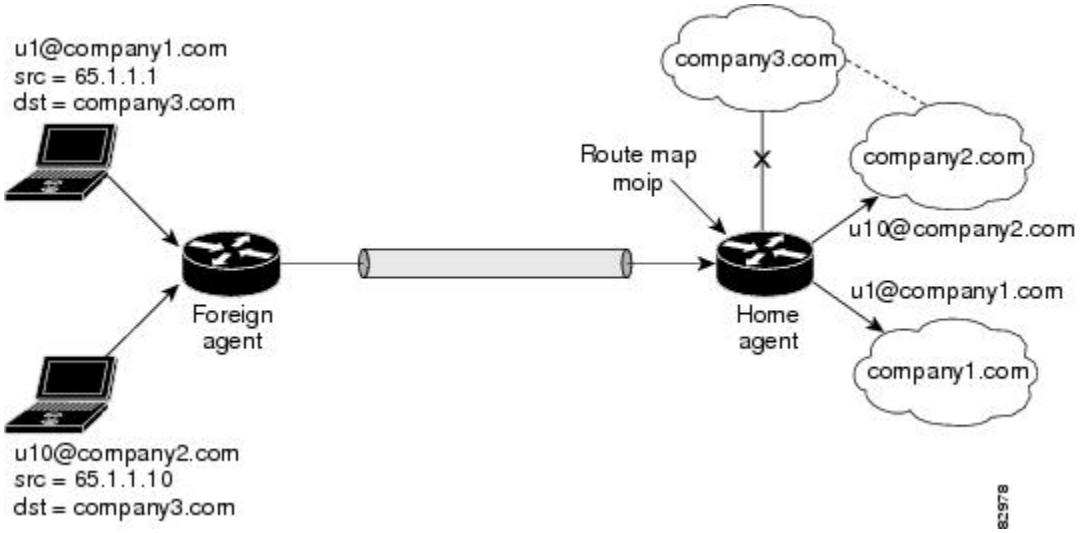
Feature Design of Mobile IP Home Agent Policy Routing

The Mobile IP Home Agent Policy Routing feature allows policy routing for mobile nodes based on the NAI configuration. ISPs can use this feature to route traffic originating from different sets of users, as identified by the NAI realm name, through different Internet connections across the policy routers. When the mobile node registers, entries are added dynamically in the access list pointed to by the route map and the route map is applied to the tunnel interface.

A route map is configured and applied on the Mobile IP tunnel. When a packet arrives on a tunnel interface and policy routing is enabled on that tunnel (route map applied), the packet is checked against the access list configured on the route map.

The figure below shows a sample topology for home agent policy routing. In the figure, as traffic from u1@company1.com and u10@ company2.com is policy routed, the home agent forwards it per the policy instead of routing directly to the destination address.

Figure 8: Sample Topology for Mobile IP Home Agent Policy Routing



How to Configure Mobile IP Home Agent Policy Routing

Enabling Policy Routing on the Home Agent

This section describes how to enable policy routing on the home agent:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **exit**
5. **ip mobile home-agent** [**address** *ip-address*]
6. **ip mobile tunnel route-map** *map-tag*
7. **ip mobile vpn-realm** *realm-name* **route-map-sequence** *sequence-number*
8. **ip mobile virtual-network** *addr mask*
9. **ip mobile host nai** *string*
10. **ip mobile secure host nai** *string* **spi** *spi* **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 5	**ip mobile home-agent** [**address** *ip-address*] **Example:** `Router(config)# ip mobile home-agent`	Enables and controls home agent services on the router.
Step 6	**ip mobile tunnel route-map** *map-tag* **Example:** `Router(config)# ip mobile tunnel route-map moipmap`	Applies the route map to the tunnel. • The *map-tag* argument must match that specified in the **route-map** *map-tag* command.
Step 7	**ip mobile vpn-realm** *realm-name* **route-map-sequence** *sequence-number* **Example:** `Router(config)# ip mobile vpn-realm corp.com route-map-sequence 20`	Defines the VPN realms to be used in home agent policy routing. • The *sequence-number* argument must match that configured in the **route-map** *sequence-number* command. The allowed sequence number range is from 0-65535.

	Command or Action	Purpose
Step 8	**ip mobile virtual-network** *addr mask* **Example:** `Router(config)# ip mobile virtual-network 10.2.0.0 255.255.0.0`	Inserts a virtual network for mobile nodes in the routing table. • This command allows the mobile nodes to use the virtual network as their home network.
Step 9	**ip mobile host nai** *string* **Example:** `Router(config)# ip mobile host nai corp.com`	Configures a mobile host, which is identified by the NAI.
Step 10	**ip mobile secure host nai** *string* **spi** *spi* **key hex** *string* **Example:** `Router(config)# ip mobile secure host nai corp.com spi 100 key hex 12345678123456781234567812345678`	Specifies the mobility security associations for the mobile host.

Defining the Route Map

This section describes how to define the route map and define the criteria by which packets are examined to learn if they will be policy-routed.

Note The Mobile IP Home Agent Policy Routing feature supports only standard access lists; named and extended access lists are not supported.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **route-map** *map-tag* [**permit** | **deny**][*sequence-number*]
4. **match ip address** *access-list-number*
5. **set interface** [*type number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables higher privilege levels, such as privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**][*sequence-number*] **Example:** `Router(config)# route-map moipmap permit 20`	Enables policy routing and enters route-map configuration mode. • The *map-tag* argument must match that specified in the **ip mobile tunnel route-map** *map-tag* command.
Step 4	**match ip address** *access-list-number* **Example:** `Router(config-route-map)# match ip address 5`	Performs policy routing on the packets. • In the example, access list 5 will be routed to the interface specified by the **set interface** command.
Step 5	**set interface** [*type number*] **Example:** `Router(config-route-map)# set interface ethernet 0`	Indicates where to output packets that pass a match clause of route map for policy routing.

Verifying Policy Routing on the Home Agent

To verify the home agent policy routing configuration, use the following commands in privileged EXEC mode, as needed:

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding**
3. **show ip mobile tunnel**
4. **show access-lists**
5. **show ip policy**
6. **show ip mobile vpn-realm**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip mobile binding** **Example:** `Router# show ip mobile binding`	Displays the mobility binding table. • See the display output in the Output Examples, on page 97 section.
Step 3	**show ip mobile tunnel** **Example:** `Router# show ip mobile tunnel`	Displays the active tunnels. • See the display output in the Output Examples, on page 97 section.
Step 4	**show access-lists** **Example:** `Router# show access-lists`	Displays the contents of the current access lists. • See the display output in the Output Examples, on page 97 section.
Step 5	**show ip policy** **Example:** `Router# show ip policy`	Displays the route map used for policy routing. • The route maps applied to the tunnels are displayed. See the display output in the Output Examples, on page 97 section.
Step 6	**show ip mobile vpn-realm** **Example:** `Router# show ip mobile vpn-realm`	Displays the Mobile IP VPN realms and sequence numbers. • See the display output in the Output Examples, on page 97 section.

Output Examples

This section provides the following output examples:

Sample Output for the show ip mobile binding Command

The following is example output for a mobile host using the NAI realm of u10@company2.com:

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
```

```
u10@company2.com (Bindings 1):
    Home Addr 65.1.1.10
    Care-of Addr 4.4.4.3, Src Addr 3.3.3.3
    Lifetime granted 00:05:00 (300), remaining 00:03:58
    Flags sBdmgvT, Identification BF7A951C.28FA35AB
    Tunnel1 src 150.150.150.150 dest 4.4.4.3 reverse-allowed
    Routing Options - (T)Reverse-tunnel
```

Sample Output for the show ip mobile tunnel Command

The following example displays the active Mobile IP tunnels and the configured route map:

```
Router# show ip mobile tunnel
Total mobile ip tunnels 1
Tunnel1:
    src 150.150.150.150, dest 4.4.4.3
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1514 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Mobile0
    HA created, fast switching enabled, ICMP unreachable enabled
    10 packets input, 1000 bytes, 0 drops
    5 packets output, 600 bytes
    Route Map is:moipmap
```

Sample Output for the show access-lists Command

The following example displays the access list:

```
Router# show access-lists
Standard IP access list 5
    permit 65.1.1.10
```

Sample Output for the show ip policy Command

The following example displays the route maps applied to the tunnels:

```
Router# show ip policy
Interface      Route map
Tunnel0        moipmap
Tunnel1        moipmap
```

Sample Output for the show ip mobile vpn-realm Command

The following examples show two VPN realms configured on the router with the corresponding **show** output:

```
ip mobile vpn-realm company1.com route-map-sequence 20
ip mobile vpn-realm company2.com route-map-sequence 10
Router# show ip mobile vpn-realm
IP Mobile VPN realm(s):
    Sequence number: 20      Realm: company1.com
    Sequence number: 10      Realm: company2.com
```

Configuration Examples for Mobile IP Home Agent Policy Routing

Home Agent Policy Routing Example

In the following example, the route map named moipmap is applied to the Mobile IP tunnel and traffic is routed, based on the NAI VPN realm configuration, through different connections across the policy routers:

```
!
router mobile
!
ip mobile home-agent address 150.150.150.150 lifetime 65535 replay 255
ip mobile vpn-realm company2.com route-map-sequence 10
ip mobile virtual-network 65.0.0.0 255.0.0.0
ip mobile host nai u10@company2.com address 65.1.1.10 virtual-network 65.0.0.0 255.0.0.0
ip mobile host nai u9@company2.com address 65.1.1.9 virtual-network 65.0.0.0 255.0.0.0
ip mobile host nai u2@company1.com address 65.1.1.2 virtual-network 65.0.0.0 255.0.0.0
ip mobile host nai u1@company1.com address 65.1.1.1 virtual-network 65.0.0.0 255.0.0.0
ip mobile secure host nai u2@company1.com spi 100 key hex 12345678123456781234567812345678
ip mobile secure host nai u1@company1.com spi 100 key hex 45678123451234567812367812345678
ip mobile secure host nai u9@company2.com spi 100 key hex 81234567812345678123456712345678
ip mobile secure host nai u10@company2.com spi 100 key hex 23456781234567812345678123456781
ip mobile tunnel route-map moipmap
!
access-list 5 permit 65.1.1.10
!
route-map moipmap permit 10
 match ip address 5
 set interface Ethernet4/4
!
```

Note This configuration example shows mobile hosts configured with static IP addresses. Mobile IP policy routing can also be used with dynamically assigned IP addresses. For example, hosts from two different NAI realms can be assigned addresses from the same address pool.

Additional References

For additional information related to Mobile IP home agent policy routing, refer to the following references:

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the *Cisco IOS IP Configuration Guide,* Release 12.2
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2

Related Topic	Document Title
Policy routing configuration tasks	"Configuring IP Routing Protocol-Independent Features" chapter in the *Cisco IOS IP Configuration Guide,* Release 12.2
Policy routing commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"IP Routing Protocol-Independent Commands" chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols,* Release 12.2
Mobile IP commands related to NAI	"Mobile IP--Generic NAI Support and Home Address Allocation" feature document, Release 12.2(13)T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

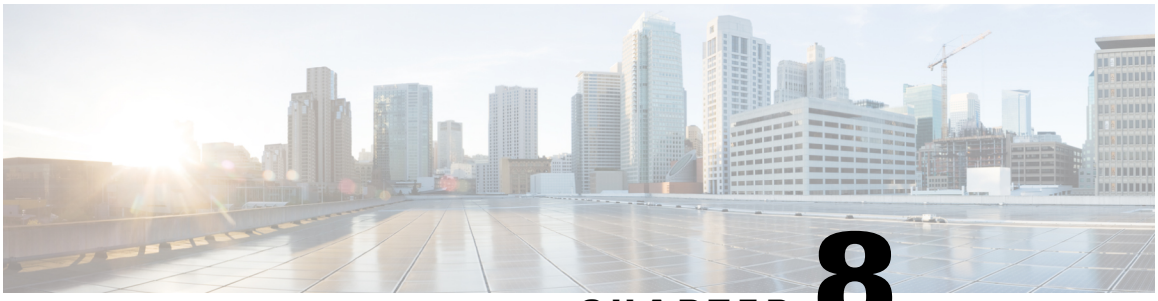
- **ip mobile tunnel**
- **ip mobile vpn-realm**
- **show ip mobile tunnel**
- **show ip mobile vpn-realm**

Glossary

home agent --A router that forwards to mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding.

NAI --network access identifier. The user ID submitted by the mobile node during registration to identify the user for authentication. The NAI may help route the registration request to the right Home Agent.

Note Refer to the Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 8

Mobile IP Home Agent Accounting

In Cisco IOS Mobile IP, the home agent keeps track of the location of the mobile node as it roams away from its home network and forwards all traffic destined to the mobile node to its new location on the Internet. The Mobile IP--Home Agent Accounting feature allows the home agent to generate the following three new accounting messages that are forwarded to the authentication, authorization, and accounting (AAA) server or the Service Selection Gateway (SSG):

- Accounting Start
- Accounting Update
- Accounting Stop

The SSG can act as the proxy server for the AAA server and acknowledge the accounting messages sent by the home agent. The accounting records generated by the home agent can be stored on the AAA server and be used by Internet service providers (ISPs) for billing, capacity planning, and operations.

Feature Specifications for the Mobile IP: Home Agent Accounting Feature

Feature History	
Release	Modification
12.2(15)T	This feature was introduced.
Supported Platforms	
For platform supported in Cisco IOS Release 12.2(15)T consult Cisco Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Mobile IP Home Agent Accounting

Because home agent accounting generates messages for the AAA server, the network should have a reachable AAA server or SSG.

Information About Mobile IP Home Agent Accounting

Service Selection Gateway

The SSG is a switching solution for service providers that offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines (DSL), cable modems, or wireless to allow simultaneous access to network services.

The SSG communicates with the AAA management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the ISP network, which may connect to the Internet, corporate networks, and value-added services.

SSG is designed and deployed such that all network traffic passes through it.

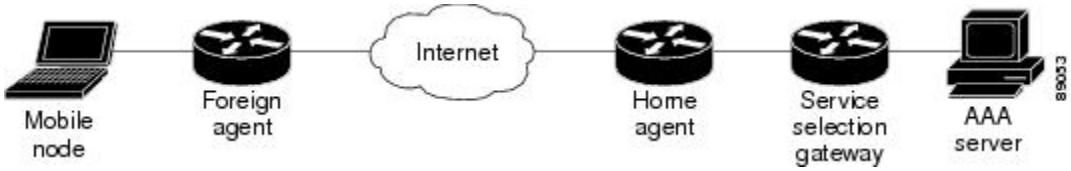
Feature Design of Home Agent Accounting

The SSG collects all the statistics information because all network traffic passes through it. However, it does not have the Mobile IP session information that the home agent maintains. The session information tracks how long a mobile node session lasts.

Note This feature was developed for the SSG to act as the proxy server for the AAA. However, this feature works equally well without the SSG and any standard AAA server can accept home agent accounting messages.

For each mobile node, the home agent sends this session information to the SSG in the form of messages, which are described in the following sections. The SSG forwards the messages to the AAA server as shown in the figure below.

Figure 9: Topology for Home Agent Accounting with SSG and AAA Server



Message Types

The following messages are sent from the home agent to the SSG or AAA server:

Accounting Start

The home agent sends an Accounting Start message to the SSG/AAA when a mobile node successfully registers for the first time. This indicates the start of a new Mobile IP session for a mobile node.

In the case of a redundant home agent, a standby home agent will send an Accounting Start message only when it becomes active and does not have any bindings. This allows the SSG to maintain host objects for mobile nodes on the failed home agent.

Accounting Update

The home agent generates an Accounting Update message when the mobile node changes its point of attachment (POA) in the mobile network. For a Mobile IP session, this corresponds to a successful re-registration from a mobile node when it changes its care-of address (CoA). The CoA is the current location of the mobile node on the foreign network.

Accounting Stop

The home agent sends an Accounting Stop message to indicate that the Mobile IP session has ended. This occurs when the lifetime of the mobile node expires, when the mobile node sends a successful deregisration request, or when the home agent is unconfigured by a network administrator.

Message Formats

All the messages contain only the following information:

- Network access identifier (NAI). This field is the name of the mobile node. The NAI is a character string that can be a unique identifier (username@realm) or a group identifier (realm).
- Network access server (NAS) IP. This field is the IP address of the accounting node. The home agent is the accounting node, so this field contains the home agent address.
- Framed IP address. This field is the IP address of the mobile node. Typically, the home agent will allocate an IP address to a mobile node after successful registration.
- Point of attachment (POA). This field indicates the POA for the mobile node on the network. For a Mobile IP session, this is the care-of address of the mobile node.

The message format is shown in the table below, including the RADIUS attribute number, which is transparent to the Mobile IP--Home Agent Accounting feature.

Table 3: Accounting Record Attributes

RADIUS Attribute Number	Attribute	Description
1	NAI/User-Name	Mobile node user name.
4	NAS IP Address	Accounting node IP address
8	Framed IP Address	IP address of the mobile node.
66	Tunnel-Client-Endpoint	This attribute is used to indicate POA/CoA address, because there is no CoA attribute. This choice of attribute works because the Mobile IP tunnel terminates on the CoA/POA and qualifies as Tunnel-Client-Endpoint.
40, 2	Acct_status_type	Indicates the accounting Start/Stop/Update for the service.

Benefits of Home Agent Accounting

The Mobile IP--Home Agent Accounting feature allows ISPs to bill consumers based on the usage of the service. The accounting information is stored on a AAA server database and used by billing software to charge for service usage for each mobile node. The ISPs can use this accounting information for billing, capacity planning, and operations.

How to Configure Mobile IP Home Agent Accounting

Configuring AAA

Access control is the way you manage who has user access to the network server and what services the users are allowed to use. AAA network security services provide the primary framework through which you set up access control on your router or access server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa accounting network** {**default** | *list-name*} **start-stop group** *group-name*
5. **aaa accounting update newinfo**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA access control.
Step 4	**aaa accounting network** {**default** | *list-name*} **start-stop group** *group-name* **Example:** `Router(config)# aaa accounting network mylist start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes. • This command creates an accounting method list for network accounting and instructs the home agent to send network events for Mobile IP. The method list can be of any name or default. • The **start-stop** keyword indicate that the home agent will send Start and Stop records to the SSG or AAA server.
Step 5	**aaa accounting update newinfo** **Example:** `Router(config)# aaa accounting update newinfo`	Enables periodic interim accounting records to be sent to the accounting server. • This command instructs the home agent to send an Accounting Update message to the SSG or AAA server when a mobile node changes its POA and acquires a new care-of address.

Configuring RADIUS

RADIUS is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {**hostname** | *ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*]
4. **radius-server retransmit** *retries*
5. **radius-server key** {0 *string* |7 *string* | *string*}
6. **radius-server attribute 44 include-in-access-req**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {**hostname**	*ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 128.107.162.173 auth-port 1645 acct-port 1646`	Specifies a RADIUS server host.
Step 4	**radius-server retransmit** *retries* **Example:** `Router(config)# radius-server retransmit 3`	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
Step 5	**radius-server key** {0 *string* |7 *string*	*string*} **Example:** `Router(config)# radius-server key cisco`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

	Command or Action	Purpose
Step 6	**radius-server attribute 44 include-in-access-req** **Example:** `Router(config)# radius-server attribute 44 include-in-access-req`	(Optional) Sends RADIUS attribute 44 in access-request packets.

Enabling Home Agent Accounting

To enable home agent accounting, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile home-agent accounting** {**default** | *list-name*}
4. **ip mobile home-agent address** *ip-address*
5. **ip mobile host** {*lower*[*upper*] | **nai** *string*} {**interface** *name*}
6. **ip mobile secure** {**host** {*lower-address*[*upper-address*]| **nai** *string*} **spi** *spi* **key hex** *string* **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix**
7. **end**
8. **show ip mobile globals**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile home-agent accounting** {**default**	*list-name*}	Enables home agent accounting.

	Command or Action	Purpose
	Example: `Router(config)# ip mobile home-agent accounting mylist`	• Applies the method list defined in the **aaa accounting** command.
Step 4	**ip mobile home-agent address** *ip-address* **Example:** `Router(config)# ip mobile home-agent address 10.3.3.1`	Enables and controls home agent services.
Step 5	**ip mobile host** {*lower*[*upper*] | **nai** *string*} {**interface** *name*} **Example:** `Router(config)# ip mobile host 10.3.3.2 10.3.3.5 interface ethernet2/2`	Configures the mobile node or mobile host group.
Step 6	**ip mobile secure** {**host** {*lower-address*[*upper-address*]| **nai** *string*} **spi** *spi* **key hex** *string* **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix** **Example:** `Router(config)# ip mobile secure host 10.3.3.2 spi 1000 key hex 12345678123456781234567812345678 algorithm md5 mode prefix-suffix`	Specifies the mobility security associations for the mobile host.
Step 7	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 8	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	Displays global information for mobile agents. • See the display output in the Examples section. Notice that the HA accounting field shows enabled status.

Examples

The following sample output shows the home agent accounting status:

```
Router# show ip mobile globals
IP Mobility global information:
Home Agent
    Registration lifetime: INFINITE
    Broadcast enabled
    Replay protection time: 10 secs
    Reverse tunnel enabled
```

```
    ICMP Unreachable enabled
    Strip realm disabled
    NAT detect disabled
    HA Accounting enabled using method list: mylist
    Address 10.3.3.1
Foreign Agent is not enabled, no care-of address
Mobility Agent
1 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled
Discovered tunnel MTU aged out after 1:00:00
```

Troubleshooting Tips

In the event that home agent accounting is not operating correctly, use the following **debug** commands in privileged EXEC mode to determine where the problem may exist:

- **debug aaa accounting**
- **debug radius**
- **debug ip mobile**

See the *Cisco IOS Debug Command Reference* publication for information about these commands.

Configuration Examples for Mobile IP Home Agent Accounting

Home Agent Accounting Example

In the following example, an accounting method list called *mylist* is created for network accounting. The accounting method list, *mylist* , is applied at the home agent, which enables home agent accounting.

```
!
aaa new-model
!
!
aaa accounting mylist start-stop group radius
aaa accounting update newinfo
!
!
ip mobile home-agent accounting mylist address 10.3.3.1
ip mobile host 10.3.3.2 10.3.3.5 interface Ethernet2/2
ip mobile secure host 10.3.3.2 spi 1000 key hex 12345678123456781234567812345678 algorithm
 md5 mode prefix-suffix
!
!
radius-server host 128.107.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
```

Additional References

For additional information related to Mobile IP--Home Agent Accounting feature, refer to the following references:

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the*Cisco IOS IP Configuration Guide,* Release 12.2
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2T
AAA configuration tasks	*Cisco IOS Security Configuration Guide,* Release 12.2
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference,* Release 12.2T
RADIUS configuration tasks	*Cisco IOS Security Configuration Guide,* Release 12.2
RADIUS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference,* Release 12.2T
SSG configuration tasks and commands	"*Service Selection Gateway* " feature document, Release 12.2(8)T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **ip mobile home-agent accounting**
- **show ip mobile globals**

Glossary

care-of address --The termination point of the tunnel to a mobile node or mobile router. This can be a collocated care-of address, by which the mobile node or mobile router acquires a local address and detunnels its own packets, or a foreign agent care-of address, by which a foreign agent detunnels packets and forwards them to the mobile node or mobile router. The care-of address is included in the Mobile IP registration request and is used by the home agent to forward packets to the mobile node in its current location.

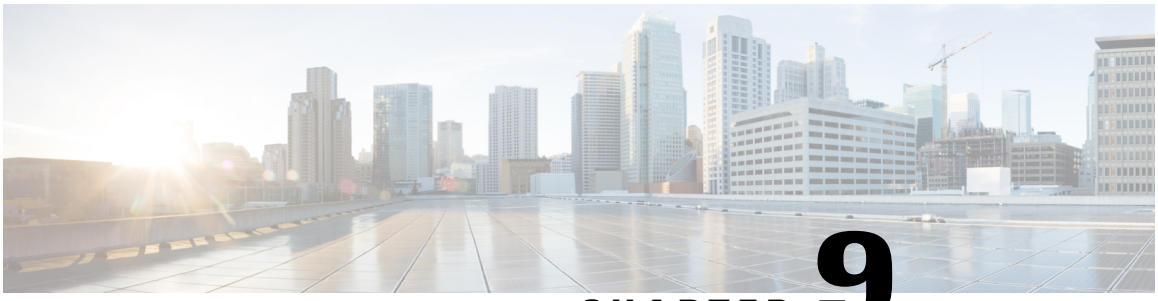
foreign agent --A router on the visited network of a foreign network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers packets to the mobile node or mobile router that were tunneled by the home agent of the mobile node. For packets sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding.

mobile node --A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming that link-layer connectivity to a point of attachment is available.

NAI --Network access identifier. The user ID submitted by the mobile node during registration to identify the user for authentication. The NAI may help route the registration request to the correct home agent.

Note Refer to the Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 9

Mobile IP Dynamic Security Association and Key Distribution

The Mobile IP Dynamic Security Association and Key Distribution feature enables a Mobile IP client (mobile node) to use the Microsoft Windows login information to generate the dynamic shared keys needed to create the security associations between it and the home agent. These security associations are used to authenticate the mobile device. In response to a successful registration, basic configuration parameters such as the DHCP server address, home address prefix length, and domain name system (DNS) address are also passed on to the mobile node in the form of extensions to the registration reply message sent by the home agent.

This feature eliminates the need for any configuration of the Mobile IP client software once it is installed. Now customers need not log in and authenticate multiple times, making the Mobile IP client software a "plug-and-play" operation.

Feature History for the Mobile IP Dynamic Security Association and Key Distribution Feature

Release	Modification
12.3(4)T	This feature was introduced.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Mobile IP Dynamic Security Association and Key Distribution

Your network must be configured to run Mobile IP. The home agent must be configured with the authentication, authorization, and accounting (AAA) address of a RADIUS server that has access to the domain controller for authenticating the user in the Windows domain.

Because Mobile IP requires support on the host device, each mobile node must be appropriately configured for the desired Mobile IP service with client software.

Restrictions for Mobile IP Dynamic Security Association and Key Distribution

This feature can be used only in a Windows operating system environment.

Information About Mobile IP Dynamic Security Association and Key Distribution

Session Identifiers

This feature introduces the concept of a session identifier (session-id) that is available if a network access identifier (NAI) is specified in your configuration. The session identifier is optional and can be added by the mobile node in the initial registration request. For example, a single user can have multiple sessions (for example when logging through different devices such as a PDA, cellular phone, or laptop) and use the same NAI for all sessions. These individual sessions are identified by the session identifier. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from the mobile node.

Using the Cisco Secure ACS Server

Because this feature leverages an existing authentication infrastructure, such as the Windows Domain Controller (DC) database or Active Directory (AD), you need not configure any Mobile IP client user information in a AAA server. You only need to configure the AAA so it can use the DC/AD to authenticate the Mobile IP client users upon receiving a RADIUS request from a home agent.

The following is a brief summary of the steps necessary to configure the Cisco Secure Access Control Server (ACS) to use a database to authenticate Mobile IP clients.

- In the navigation bar, click External User Databases. Select Windows Domain Database to authenticate unknown users.
- In the navigation bar, click External User Databases. Map the domain of the unknown users to an ACS group.
- Click Database Group Mappings. Check the Microsoft MPPE Key attribute for the mapped ACS group.

For more information on Cisco Secure ACS configuration, refer to the "Administering External User Databases" chapter of the *Cisco Secure ACS Windows Server 3.1 User Guide*.

Benefits of Mobile IP Dynamic Security Association and Key Distribution

- This feature eliminates the need for any configuration of the Mobile IP client software once it is installed. Now customers need not log in and authenticate multiple times, making the Mobile IP client software a "plug-and-play" operation.
- For network administrators, this feature simplifies Mobile IP provisioning and increases mobility security through dynamic re-keying.

Additional References

The following sections provide references related to the Mobile IP Dynamic Security Association and Key Distribution feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility,* Release 12.3 T
Information about Network Access Identifiers in Mobile IP	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnaiadd.htm Mobile IP Generic NAI Support and Home Address Allocation feature document, Release 12.2(13)T

Related Topic	Document Title
Configuration tasks for Cisco Secure ACS	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs31/acsuser/acs31ug.pdf Cisco Secure ACS Windows Server 3.1 User Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **clear ip mobile binding**
- **clear ip mobile visitor**
- **show ip mobile binding**
- **show ip mobile visitor**

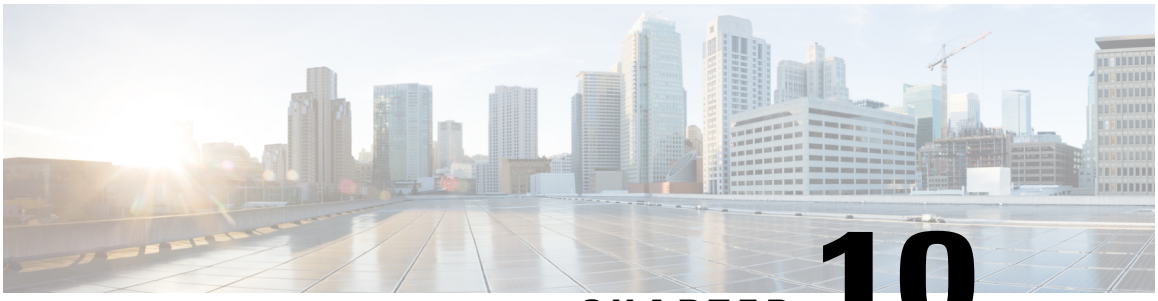
Glossary

home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while it is away from home. It keeps current location information for registered mobile nodes called a mobility binding.

mobile node --A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming that link-layer connectivity to a point of attachment is available.

NAI--network access identifier. The user ID submitted by the mobile node during registration to identify the user for authentication. The NAI might help route the registration request to the correct home agent.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 10

Mobile IP Support for RFC 3519 NAT Traversal

The Mobile IP: Support for RFC 3519 NAT Traversal feature introduces an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added for establishing User Datagram Protocol (UDP) tunneling.

The benefit of this feature is that mobile devices in collocated mode that use a private IP address (RFC 1918) or foreign agents (FAs) that use a private IP address for the care-of address (CoA) are now able to establish a tunnel and traverse a NAT-enabled router with mobile node (MN) data traffic from the home agent (HA).

Feature History for Mobile IP: Support for RFC 3519 NAT Traversal

Release	Modification
12.3(8)T	This feature was introduced.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Mobile IP Support for RFC 3519 NAT Traversal

- If the network does not allow communication between a UDP port chosen by an MN and the HA UDP port 434, the Mobile IP registration and the data tunneling will not work.
- Only the IP-to-UDP encapsulation method is supported.

Information About Mobile IP Support for RFC 3519 NAT Traversal

Design of the Mobile IP Support for RFC 3519 NAT Traversal Feature

Because of the depletion of globally routable addresses, service providers and enterprises are using addresses from private- and public-address realms and are using NAT-based solutions for achieving transparent routing between these address realms. Private IP addresses (RFC 1918) allow each enterprise to use the same addresses except that the addresses cannot be seen in the Internet outside of the enterprise or service provider network.

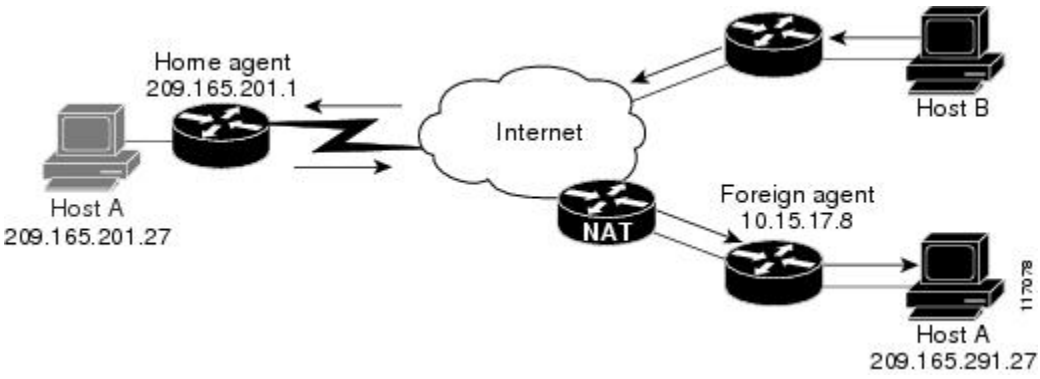
Network Address Translation (NAT) allows for the translation of a private IP address to a public IP address. NAT uses the port number in the second header to organize the translations and determine which translation (if any) to use when it sees a returning packet.

The Mobile IP: Support for RFC 3519 NAT Traversal feature uses new message extensions in registration packets to establish UDP tunneling. When the MN registration packet traverses a NAT-enabled router, the HA detects the traversal by comparing the source IP address with the CoA and establishes UDP tunneling if the MN indicates that it is capable of UDP tunneling. The MN indicates the UDP tunneling capability by including the UDP tunneling extension in the registration request.

The NAT-enabled router allows the UDP registration packet to proceed through. UDP tunneling allows data packets from the HA to use the NAT translation set up by the registration packet. This occurs because the UDP tunnel header uses the same UDP source and destination port as the original registration packet, thus allowing it to use the NAT translation created for and by the registration packet traversing the NAT-enabled router. This allows the MN to receive data packets from the HA when it normally would not with the default IPinIP tunneling.

The figure below shows Mobile IP components and their relationships.

Figure 10: Mobile IP Components and Relationships



Note UDP tunneling is the only method that supports NAT traversal in Mobile IP.

Network Address Translation Devices

Network Address Translation (NAT) devices rely on IP addresses and port numbers from IP, TCP, and UDP layers for demultiplexing data to peers behind a NAT network. When a message is initiated from a private-address host to a public-address host, NAT modifies the source IP address in the packet to a globally routable source address and the source port number to a unique source port number that it can use for identifying the peer that initiates the message. NAT then preserves the private address, port-to-public address, and port mapping in its translation table and uses the NAT-translation entry to route the return traffic.

The Mobile IP: Support for RFC 3519 NAT Traversal feature provides UDP tunneling for data packets so that NAT devices can translate the IP addresses and forward the data packets from the HA to the MN.

UDP Tunneling

There are two directions for UDP tunneling: forward and reverse. Forward tunneling is done by an HA that forwards packets towards the MN, and reverse tunneling starts at the MN care-of address and terminates at the HA.

UDP tunneled packets that have been sent by an MN use the same ports as the registration request message. In particular, the source port may vary between new registration requests, but remains the same for all tunneled data and reregistrations. The destination port is always 434. UDP tunneled packets that are sent by an HA use the same ports, but in reverse.

Note UDP tunneling is for Mobile IP data traffic only. Registration requests and replies do not use UDP tunneling.

By setting the force bit in the UDP tunneling request, the MN can request Mobile IP UDP tunneling be established regardless of the NAT detection outcome by the HA. The final outcome of whether or not the MN will receive UDP tunneling is determined by whether or not the HA is configured to accept such requests.

Keepalive Management

The purpose of the keepalive messages is to refresh the active timer on the NAT translation in the NAT-enabled router. This maintains the NAT translation for use by the HA even when the MN is silent. This allows data packets from the HA to use the NAT translation created by the registration packet to traverse the NAT-enabled router and reach the MN even when the MN may not be sending any packets to the HA to keep the NAT translation active.

The keepalive timer interval is configurable on both the HA and the FA but is controlled by the HA keepalive interval value sent in the registration reply. When the HA sends a keepalive value in the registration reply, the MN or FA must use that value as its keepalive timer interval.

The keepalive interval configured on the FA is only used if the HA returns a keepalive interval of zero in the registration reply.

Note You cannot configure the HA to send a keepalive interval value of zero the FA or MN.

New Message Extensions

An extension is added to the end of a registration packet and indicates that it is a type, length, value (TLV) message. RFC 3519 discusses the UDP tunnel request and reply extension and a Mobile IP tunnel data message that serves to differentiate traffic tunneled to port 434.

The Mobile IP--Support for RFC 3519 NAT Traversal feature adds the following new UDP tunnel message extensions:

- Request--This message extension indicates that the sender is capable of handling UDP tunneling. Some encapsulation formats are optional.
- Reply--This message extension indicates whether or not the HA will use UDP tunneling. The HA also sends the keepalive interval in the reply message.
- Mobile IP tunnel data--This message extension is used to differentiate UDP data traffic tunneled to port 434 from other Mobile IP messages that use a UDP header such as registration requests.

UDP Tunnel Flag

The Mobile IP--Support for RFC 3519 NAT Traversal feature adds a new UDP tunnel flag in the agent advertisement that indicates the capability of the FA to support NAT traversal. The flag is a bit set in the advertisement.

How to Configure Mobile IP Support for RFC 3519 NAT Traversal

Configuring the Home Agent for NAT Traversal Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile home-agent nat traversal [keepalive keepalive-time] [forced {accept | reject}]**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile home-agent nat traversal [keepalive keepalive-time] [forced {accept | reject}]** **Example:** `Router(config)# ip mobile home-agent nat traversal keepalive 45 forced accept`	Enables UDP tunneling for an HA. The keywords and argument are as follows: • **keepalive** *keepalive-time* --(Optional) Time, in seconds, between keepalive messages that are sent between UDP endpoints to refresh NAT translation timers. The range is 0 to 65535. The default is 110. You cannot configure the HA to send a zero as the keepalive timer to the FA or MN. • **forced** --(Optional) Enables the HA to accept or reject forced UDP tunneling from the MN regardless of the NAT-detection outcome. • **accept**--Accepts UDP tunneling. • **reject**--Rejects UDP tunneling. This is the default. **Note** If the **forced** keyword is not specified, the command defaults to reject UDP tunneling.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the Foreign Agent for NAT Traversal Support

This task shows you how to configure the FA for NAT traversal support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**] **Example:** `Router(config)# ip mobile foreign-agent nat traversal keepalive 45 force`	Enables UDP tunneling for the FA. The keywords and argument are as follows: • **keepalive** *keepalive-time* --(Optional) Allows the FA to use a configured time (in seconds) for keepalive messages when the HA keepalive time is not configured. The range is 0 to 65535. The default is 110. **Note** The Cisco HA will never send a time of zero. If you have Cisco hardware only, you do not need to configure the **keepalive** keyword.

	Command or Action	Purpose
		• **force** --(Optional) Sets the "force" bit in the message extension. The default is not to force UDP tunneling.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying NAT Traversal Support

SUMMARY STEPS

1. **show ip mobile globals**
2. **show ip mobile binding**
3. **show ip mobile visitor**
4. **show ip mobile tunnel**
5. **debug ip mobile**

DETAILED STEPS

Step 1 **show ip mobile globals**

Use this command to verify the FA and HA configurations, for example:

Example:

```
Router# show ip mobile globals
IP Mobility global information:
Home agent
 Registration lifetime: 10:00:00 (36000 secs)
 Broadcast disabled
 Replay protection time: 7 secs
 Reverse tunnel enabled
 ICMP Unreachable enabled
 Strip realm disabled
 NAT Traversal disabled
 HA Accounting disabled
 NAT UDP Tunneling support enabled
 UDP Tunnel Keepalive 60
 Forced UDP Tunneling enabled
 Virtual networks
 10.99.101.0/24
Foreign agent is not enabled, no care-of address
0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
```

In the example above, NAT UDP tunneling support is enabled on the HA with a keepalive timer set at 60 seconds and forced UDP tunneling enabled.

Step 2 **show ip mobile binding**

Use this command to verify that the HA is configured to detect NAT, for example:

Example:

```
Router# show ip mobile binding nai mn@cisco.com
Mobility Binding List:
 mn@cisco.com (Bindings 1):
 Home Addr 10.99.101.1
 Care-of Addr 192.168.1.202, Src Addr 209.165.157
 Lifetime granted 00:03:00 (180), remaining 00:02:20
 Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
 Tunnel0 src 209.165.202.1 dest 209.165.157 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Service Options:
 NAT detect
```

Step 3 **show ip mobile visitor**

Use this command to verify that the MN is registering with the HA (at the FA), for example:

Example:

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
10.99.100.2:
 Interface FastEthernet3/0, MAC addr 00ff.ff80.002b
 IP src 10.99.100.2, dest 30.5.3.5, UDP src port 434
 HA addr 200.1.1.1, Identification BCE7E391.A09E8720
 Lifetime 01:00:00 (3600) Remaining 00:30:09
 Tunnel1 src 200.1.1.5, dest 200.1.1.1, reverse-allowed
 Routing Options - (T)Reverse Tunneling
```

Step 4 **show ip mobile tunnel**

Use this command to verify that UDP tunneling is established, for example:

Example:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
    src 10.30.30.1, dest 10.10.10.100
    src port 434, dest port 434
    encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/3
    FA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    7 packets output, 780 bytes
```

The following output shows that the mobile node-home agent tunnel is still IP-in-IP, but the foreign agent-home agent tunnel is UDP, for example:

Example:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
 src 200.1.1.1, dest 10.99.100.2
 encap IP/IP
, mode reverse-allowed, tunnel-users 1
 IP MTU 1460 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Tunnel1
 HA created, fast switching enabled, ICMP unreachable enabled
 11 packets input, 1002 bytes, 0 drops
 5 packets output, 600 bytes
Tunnel1:
 src 200.1.1.1, dest 200.1.1.5
 src port 434, dest port 434
 encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface GigabitEthernet0/2
 HA created, fast switching disabled, ICMP unreachable enabled
 11 packets input, 1222 bytes, 0 drops
 7 packets output, 916 bytes
```

In the following example, the MN has UDP tunneling established with the HA, for example:

Example:

```
Router# show ip mobile tunnel
Total mobile ip tunnels 1
Tunnel0:
    src 10.10.10.100, dest 10.10.10.50
    src port 434, dest port 434
    encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/1
    HA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    5 packets output, 600 bytes
```

Step 5 **debug ip mobile**

Use this command to verify the registration, authentication, and establishment of UDP tunneling of the MN with the FA (important lines in bold), for example:

Example:

```
Dec 31 12:34:25.707: UDP: rcvd src=10.10.10.10(434),dst=10.30.30.1(434), length=54
Dec 31 12:34:25.707: MobileIP: ParseRegExt type MHAE(32) addr 2000FEEC end 2000FF02
Dec 31 12:34:25.707: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.707: MobileIP: FA rcv registration for MN 10.10.10.10
 on Ethernet2/2 using  COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options sbdmg-T-identification
  C1BC0D4FB01AC0D8
Dec 31 12:34:25.707: MobileIP: Ethernet2/2 glean 10.10.10.10 accepted
Dec 31 12:34:25.707: MobileIP: Registration request byte count = 74
Dec 31 12:34:25.707: MobileIP: FA queued MN 10.10.10.10 in register table
Dec 31 12:34:25.707: MobileIP: Visitor registration timer started for MN 10.10.10.10,  lifetime 120
Dec 31 12:34:25.707: MobileIP: Adding UDP Tunnel req extension
Dec 31 12:34:25.707: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.707: MobileIP: MN 10.10.10.10 FHAE added to HA 10.10.10.100 using SPI 1000
```

```
Dec 31 12:34:25.707: MobileIP: FA forwarded registration for MN 10.10.10.10 to HA  10.10.10.100
Dec 31 12:34:25.715: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=94
Dec 31 12:34:25.715: MobileIP: ParseRegExt type NVSE(134) addr 20010B28 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MN-config NVSE(14) subtype 1 (MN prefix  length)
prefix length (24)
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 12 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MHAE(32) addr 20010B36 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 20010B4C end 20010B6A
Dec 31 12:34:25.715: Parsing UDP Tunnel Reply Extension - length 6
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type FHAE(34) addr 20010B54 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: FA rcv accept (0) reply for MN 10.10.10.10 on Ethernet2/3  using HA
10.10.10.100 lifetime 65535
Dec 31 12:34:25.719: MobileIP: Authenticating HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.719: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.719: MobileIP: Authenticated HA 10.10.10.100 using SPI 1000 and 16 byte  key
Dec 31 12:34:25.719: MobileIP: HA accepts UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Update visitor table for MN 10.10.10.10
Dec 31 12:34:25.719: MobileIP: Enabling UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.30.30.1 dst  10.10.10.100
Dec 31 12:34:25.719: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.30.30.1:0 -
10.10.10.100:0 with keep-alive 30
Dec 31 12:34:25.719: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:25.719: MobileIP: ARP entry for MN 10.10.10.10 using 10.10.10.10 inserted on  Ethernet2/2
Dec 31 12:34:25.719: MobileIP: FA route add 10.10.10.10 successful. Code = 0
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 added to ReverseTunnelTable of Ethernet2/2  (Entries
1)
Dec 31 12:34:25.719: MobileIP: FA dequeued MN 10.10.10.10 from register table
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 using 10.10.10.10 visiting on Ethernet2/2 Dec 31
12:34:25.719: MobileIP: Reply in for MN 10.10.10.10 using 10.10.10.10, accepted
Dec 31 12:34:25.719: MobileIP: registration reply byte count = 84
Dec 31 12:34:25.719: MobileIP: FA forwarding reply to MN 10.10.10.10 (10.10.10.10 mac  0060.70ca.f021)
Dec 31 12:34:26.095: MobileIP: agent advertisement byte count = 48
Dec 31 12:34:26.095: MobileIP: Agent advertisement sent out Ethernet2/2: type=16, len=10,  seq=55,
lifetime=65535, flags=0x1580(rbhFmG-TU),
Dec 31 12:34:26.095: Care-of address: 10.30.30.1
Dec 31 12:34:26.719: MobileIP: swif coming up Tunnel0
!
Dec 31 12:34:35.719: UDP: sent src=10.30.30.1(434), dst=10.10.10.100(434)
Dec 31 12:34:35.719: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=32d0
```

In the following example, the registration, authentication, and establishment of UDP tunneling of the MN with the HA is displayed:

Example:

```
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type UDPTUNREQE(144)
addr 2001E762 end 2001E780
Dec 31 12:34:26.167: MobileIP: Parsing UDP Tunnel Request Extension - length 6
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type FHAE(34) addr 2001E76A end 2001E780
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: HA 167 rcv registration for MN 10.10.10.10 on Ethernet2/1  using
HomeAddr 10.10.10.10 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options  sbdmg-T-identification
C1BC0D4FB01AC0D8
Dec 31 12:34:26.167: MobileIP: NAT detected SRC:10.10.10.50 COA: 10.30.30.1
Dec 31 12:34:26.167: MobileIP: UDP Tunnel Request accepted 10.10.10.50:434
Dec 31 12:34:26.167: MobileIP: Authenticating FA 10.30.30.1 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated FA 10.30.30.1 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticating MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
```

```
Dec 31 12:34:26.167: MobileIP: Authenticated MN 10.10.10.10 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Mobility binding for MN 10.10.10.10 created
Dec 31 12:34:26.167: MobileIP: NAT detected for MN 10.10.10.10. Terminating tunnel on  10.10.10.50
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.10.10.100 dst  10.10.10.50
Dec 31 12:34:26.167: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.10.10.100:0 -
10.10.10.50:0 with keep-alive 30
Dec 31 12:34:26.167: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 Insert route for 10.10.10.10/255.255.255.255  via
gateway 10.10.10.50 on Tunnel0
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 is now roaming
Dec 31 12:34:26.171: MobileIP: Gratuitous ARPs sent for MN 10.10.10.10 MAC 0002.fca5.bc39
Dec 31 12:34:26.171: MobileIP: Mask for address is 24
Dec 31 12:34:26.171: MobileIP: HA accepts registration from MN 10.10.10.10
Dec 31 12:34:26.171: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Dec 31 12:34:26.171: MobileIP: Composed mobile network extension length:0
Dec 31 12:34:26.171: MobileIP: Added prefix length vse in reply
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 - HA sent reply to 10.10.10.50
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: ParseRegExt type CVSE(38) addr 2000128C end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HA red. version CVSE(6)
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 8 to next
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HHAE(35) addr 20001298 end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.175: MobileIP: Authenticating HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authenticated HA 10.10.10.3 using SPI 1000 and 16 byte key
Dec 31 12:34:27.167: MobileIP: swif coming up Tunnel0d0
```

In the following example, the force option is missing on the HA configuration, so the UDP tunneling request is rejected:

Example:

```
Router# debug ip mobile
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type NVSE(134) addr C368C6C
end C368
C9C
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type dynamic mobile-network
NVSE(9)
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 16 to next
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type MHAE(32) addr C368C7E
end C368C9C
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 20 to next
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type UDPTUNREQE(144) addr
C368C94 end C368C9C
*Jun 6 20:49:28.147: MobileIP: Parsing UDP Tunnel Request Extension -
length 6
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 6 to next
*Jun 6 20:49:28.147: MobileIP: HA 143 rcv registration for MN
10.99.100.2 on Gi
gabitEthernet0/2 using HomeAddr 10.99.100.2 COA 200.1.1.5 HA 200.1.1.1
lifetime
3600 options sbdmg-T- identification BCE7E253A7CAF30C
*Jun 6 20:49:28.147: MobileIP: NAT not detected SRC:200.1.1.5 COA:
200.1.1.5
*Jun 6 20:49:28.147: MobileIP: Forced UDP Tunneling requested
*Jun 6 20:49:28.147: MobileIP: UDP Tunnel Request rejected
*Jun 6 20:49:28.147: MobileIP: HA rejects registration for MN
10.99.100.2 - registration id mismatch (133)
```

Configuration Examples for Mobile IP Support for RFC 3519 NAT Traversal

Home Agent Configuration Examples

The following example shows an active HA configuration.

```
ip mobile home-agent nat traversal keepalive 56 forced accept
ip mobile home-agent redundancy Phy1 virtual-network
ip mobile virtual-network 10.60.60.0 255.255.255.0 address 10.60.60.200
```

The following example shows a standby HA configuration.

```
ip mobile home-agent nat traversal keepalive 56 forced accept
ip mobile home-agent redundancy Phy1 virtual-network
ip mobile virtual-network 10.60.60.0 255.255.255.0 address 10.60.60.200
```

Foreign Agent Configuration Example

The following example shows the FA configuration on Ethernet interface 2/2. The FA does not use the 45-second keepalive interval unless the HA sends back a zero as the interval in the registration reply.

```
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent nat traversal keepalive 45 force
```

Firewall Configuration Example

The following example shows a configuration when a firewall is sitting between a FA and a HA. The firewall blocks IP-in-IP and GRE packets, but permits UDP packets. The HA and FA are configured to force the HA to use the UDP encapsulation.

HA Configuration

```
interface Loopback1
ip address 200.1.1.1 255.255.255.255
!
router mobile
!
! The following command set UDP keepalive interval to 60 second and enables the HA to accept
 forced UDP tunneling registration requests.
!
ip mobile home-agent nat traversal keepalive 60 forced accept
ip mobile home-agent
ip mobile virtual-network 10.99.100.0 255.255.255.0
ip mobile host 10.99.100.1 10.99.100.100 virtual-network 10.99.100.0 255.255.255.0
ip mobile mobile-networks 10.99.100.2
description MAR-3200
register
ip mobile secure host 10.99.100.1 10.99.100.100 spi 100 key hex
12345678123456781234567812345678 algorithm md5 mode prefix-suffix
```

Foreign Agent Configuration

```
interface Loopback1
ip address 10.1.1.5 255.255.255.255
!
interface FastEthernet3/0
ip address 10.5.3.5 255.255.255.0
ip irdp
ip irdp maxadvertinterval 9
ip irdp minadvertinterval 3
ip irdp holdtime 27
ip mobile foreign-service reverse-tunnel
!
ip mobile foreign-agent care-of Loopback1
!
! The following command forces the FA to request the HA to use UDP tunneling for MN. Without
 this command, the HA is configured to accept UDP tunneling. The HA will not use UDP tunneling
 if it is not NAT detected.
ip mobile foreign-agent nat traversal force
```

Mobile Router Configuration

```
interface Loopback1
!Description MR's home address.
ip address 10.99.100.2 255.255.255.255
!
interface FastEthernet0/0
description "802.11 Wi-Fi Link"
ip address 10.5.3.32 255.255.255.0
ip mobile router-service roam priority 120
!
ip mobile router
address 10.99.100.2 255.255.255.0
collocated single-tunnel
home-agent 10.1.1.1 priority 110
mobile-network Vlan210
reverse-tunnel
```

Cisco IOS Firewall

In the following example, an IP access-list is used to simulate the blocking of IP-in-IP and GRE packets.

```
!Input interface for the traffic coming from MR.
interface FastEthernet0/1
ip address 10.1.35.3 255.255.255.0
ip access-group Block-IPinIP-GRE-Packets in
!
ip access-list extended Block-IPinIP-GRE-Packets
deny ipinip any any
deny gre any any
permit ip any any
```

Additional References

The following sections provide references related to the Mobile IP--Support for RFC 3519 NAT Traversal feature.

Related Documents

Related Topic	Document Title
Generic routing encapsulation	Generic Routing Encapsulation, RFC 1701

Related Topic	Document Title
IP encapsulation	IP Encapsulation in IP, RFC 2003
Mobile IP overview and configuration	*"Configuring Mobile IP" chapter of the* Cisco IOS IP Configuration Guide , Release 12.3
Mobile IP traversal of NAT devices	Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519
Mobile IP command description and syntax	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3 T
NAT and Network Address Port Translation (NAPT) overview and configuration	• *"Configuring IP Addressing" chapter of the* Cisco IOS IP Configuration Guide , Release 12.3 • Cisco IOS IP Command Reference, Volume 1 of 4: IP Addressing and Services , Release 12.3 T • IP NAT Terminology and Considerations, RFC 2663 • Network Address Translation - Protocol Translation, RFC 2766

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **debug ip mobile**
- **ip mobile foreign-agent nat traversal**
- **ip mobile home-agent nat traversal**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile tunnel**
- **show ip mobile visitor**

Glossary

care-of address--There are two types of care-of addresses: FA care-of addresses and collocated care-of addresses. An FA care-of address is a temporary, loaned IP address that an MN acquires from an FA agent advertisement. It is the exit point of the tunnel from the HA to the FA. A collocated care-of address is an address temporarily assigned to an MN interface that is assigned by DHCP or by manual configuration.

FA --foreign agent. An FA is a router on a foreign network that assists the MN in informing its HA of its current care-of address. The FA detunnels and delivers packets to the MN that were tunneled by the HA. The FA also acts as the default router for packets generated by the MN while it is connected to the foreign network.

forward tunnel --A tunnel that forwards packets toward the mobile node. It starts at the home agent and ends at the MN care-of address.

HA --home agent. An HA is a router on the home network of an MN that maintains an association between the home IP address of the MN and its *care-of address* , which is the current location of the MN on a foreign or visited network. The HA redirects packets by tunneling them to the MN while it is away from home.

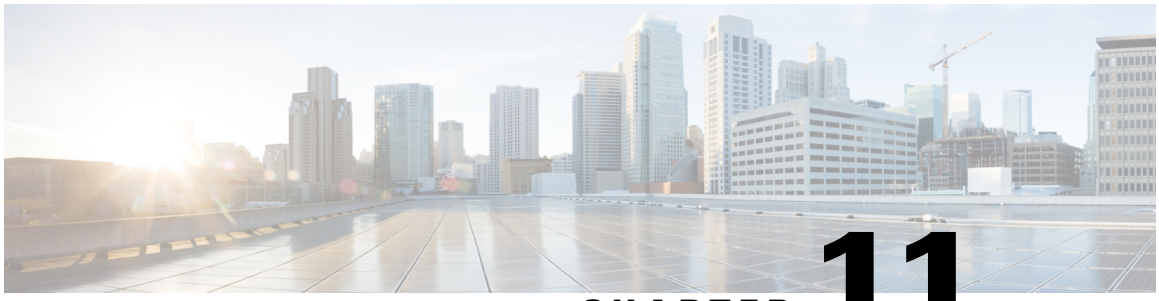
MN --mobile node. An MN is a node, for example, a PDA, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This node can maintain ongoing communications while using only its home IP address.

NAT --Network Address Translation. NAT is a mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator. Basic NAT is a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, the source IP address and related fields such as IP, TCP, UDP, and ICMP header checksums are translated. For inbound packets, the destination IP address and the checksums as listed above are translated.

NAPT --Network Address Port Translation. NAPT translates transport identifier (for example, TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of private hosts to be multiplexed into the transport identifiers of a single external address. NAPT allows a set of hosts to share a single external address. Note that NAPT can be combined with basic NAT so that a pool of external addresses are used in conjunction with port translation.

reverse tunnel --A tunnel that starts at the MN care-of address and terminates at the HA.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.



CHAPTER 11

Mobile IPv6 High Availability

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users, whether they are within their enterprise networks or away from home.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Mobile IPv6 High Availability

Mobile IPv6 Tunnel Optimization

Mobile IPv6 tunnel optimization enables routing over a native IPv6 tunnel infrastructure, allowing Mobile IPv6 to use all IPv6 tunneling infrastructure features, such as Cisco Express Forwarding switching support.

After the home agent receives a valid BU request from a mobile node, it sets up its endpoint of the bidirectional tunnel. This process involves creating a logical interface with the encapsulation mode set to IPv6/IPv6, the tunnel source to the home agent's address on the mobile node's home link, and the tunnel destination set to the mobile node's registered care-of address. A route will be inserted into the routing table for the mobile node's home address via the tunnel.

IPv6 Host Group Configuration

Users can create mobile user or group policies using the IPv6 host group configuration. The host group profile lookup interface will allow the lookup of the profile associated with the sender of the BU using any of the search keys:

- Profile name
- IPv6 address
- Network address identifier (NAI)

The host profile lookup interface also specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional security parameter index (SPI).

A group profile is activated after the SPI option is configured and either an NAI or an IPv6 address is configured. In addition, a profile is deactivated if the minimum required options are not configured. If any active profile that has active bindings gets deactivated or removed, all bindings associated to that profile are revoked.

Mobile IPv6 Node Identification Based on NAI

A mobile node can identify itself using its home address as an identifier. The Mobile IPv6 protocol messages use this identifier in their registration messages. However, for certain deployments it is essential that the mobile node has the capability to identify itself using a logical identifier, such as NAI, rather than a network address. The mobile node identifier option for Mobile IPv6 allows a mobile node to be identified by NAI rather than IPv6 address. This feature enables the network to give a dynamic IPv6 address to a mobile node and authenticate the mobile node using authentication, authorization, and accounting (AAA). This option should be used when either Internet Key Exchange (IKE) or IPsec is not used for protecting BUs or binding acknowledgments (BAs).

In order to provide roaming services, a standardized method, such as NAI or a mobile node home address, is needed for identifying users. Roaming may be loosely defined as the ability to use any one of multiple Internet service providers (ISPs) while maintaining a formal, customer-vendor relationship with only one. Examples of where roaming capabilities might be required include ISP confederations and ISP-provided corporate network access support. Other entities interested in roaming capability may include the following:

- Regional ISPs, operating within a particular state or province, that want to combine efforts with those of other regional providers to offer dialup service over a wider area.
- National ISPs that want to combine their operations with those of one or more ISPs in another country to offer more comprehensive dialup service in a group of countries or on a continent.
- Wireless LAN hot spots that provide service to one or more ISPs.
- Businesses that want to offer their employees a comprehensive package of dialup services on a global basis. Those services may include Internet access and secure access to corporate intranets using a VPN.

Authentication Protocol for Mobile IPv6

The authentication protocol for Mobile IPv6 support secures mobile node and home agent signaling using the MN-HA mobility message authentication option, which authenticates the BU and BA messages based on the shared-key-based security association between the mobile node (MN) and the HA. This feature allows Mobile IPv6 to be deployed in a production environment where a non-IPsec authentication method is required. MN-HA consists of a mobility SPI, a shared key, an authentication algorithm, and the mobility message replay protection option.

The mobility SPI is a number from 256 through 4,294,967,296. The key consists of an arbitrary value and is 16 octets in length. The authentication algorithm used is HMAC_SHA1. The replay protection mechanism may use either the sequence number option or the time-stamp option. The MN-HA mobility message authentication option must be the last option in a message with a mobility header if it is the only mobility message authentication option in the message.

When a BU or BA message is received without the MN-HA option and the entity receiving it is configured to use the MN-HA option or has the shared-key-based mobility security association for the mobility message authentication option, the entity discards the received message.

The mobility message replay protection option allows the home agent to verify that a BU has been freshly generated by the mobile node and not replayed by an attacker from some previous BU. This functionality is especially useful for cases where the home agent does not maintain stateful information about the mobile node after the binding entry has been removed. The home agent performs the replay protection check after the BU has been authenticated. The mobility message replay protection option is used by the mobile node for matching the BA with the BU. When the home agent receives the mobility message replay protection option in BU, it must include the mobility message replay protection option in the BA.

How to Configure Mobile IPv6 High Availability

Verifying Native IPv6 Tunneling for Mobile IPv6

Using the native IPv6 tunneling (or generic routing encapsulation [GRE]) infrastructure improves the scalability and switching performance of the home agent. After the home agent sends a BU from a mobile node, a tunnel interface is created with the encapsulation mode set to IPv6/IPv6, the source address set to that of the home agent address on the home interface of the mobile node, and the tunnel destination set to that of the CoA of the mobile node.

These features are transparent and need not be configured in order to work with Mobile IPv6. For further information on IPv6 tunneling and how to implement GRE tunneling in IPv6, see the *Implementing Tunneling for IPv6* module.

SUMMARY STEPS

1. **enable**
2. **show ipv6 mobile tunnels** [**summary** | **tunnel** *if-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 mobile tunnels** [**summary**	**tunnel** *if-number* **Example:** `Router# show ipv6 mobile tunnels`	Lists the Mobile IPv6 tunnels on the home agent.

Configuring and Verifying Host Groups for Mobile IPv6

Users can create mobile user or group policies using the host group configuration. The host group profile lookup interface will allow the lookup of the profile associated with the sender of the BU using the sender's profile name, IPv6 address, or NAI. The host profile lookup interface also specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.

A mobile node can identify itself using its profile name or home address as an identifier, which the Mobile IPv6 protocol messages use as an identifier in their registration messages. However, for certain deployments it is essential that the mobile node has the capability to identify itself using a logical identifier such as NAI rather than a network address.

Note

- You cannot configure two host group profiles with the same IPv6 address when using the IPv6 address option.
- You cannot configure a profile with the NAI option set to a realm name and the address option set to a specific IPv6 address. You can either remove the NAI option or specify a fully qualified user name for the NAI option.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile home-agent**
4. **binding** [**access** *access-list-name* | *auth-option* | *seconds*| *maximum* | *refresh*
5. **host group** *profile-name*
6. **address** {*ipv6-address* | **autoconfig**
7. **nai realm** | **user** | **macaddress**] {*user* **@** *realm*| **@** *realm*
8. **authentication inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds*
9. **exit**
10. **exit**
11. **show ipv6 mobile host groups** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mobile home-agent** **Example:** `Router(config)# ipv6 mobile home-agent`	Places the router in home-agent configuration mode.
Step 4	**binding** [**access** *access-list-name*	*auth-option*	*seconds*| *maximum*	*refresh* **Example:** `Router(config-ha)# binding 15`	Configures binding options for the Mobile IPv6 home agent feature.
Step 5	**host group** *profile-name* **Example:** `Router(config-ha)# host group profile1`	Creates a host configuration in Mobile IPv6. • Multiple instances with different profile names can be created and used.

	Command or Action	Purpose
Step 6	**address** {*ipv6-address* | **autoconfig** **Example:** `Router(config-ha)# address baba 2001:DB8:1`	Specifies the home address of the IPv6 mobile node.
Step 7	**nai realm** | **user** | **macaddress**] {*user* **@** *realm*| **@** *realm* **Example:** `Router(config-ha)# nai @cisco.com`	Specifies the NAI for the IPv6 mobile node.
Step 8	**authentication inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds* **Example:** `Router(config-ha)# authentication spi 500 key ascii cisco`	Specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.
Step 9	**exit** **Example:** `Router(config-ha)# exit`	Exits home-agent configuration mode, and returns the router to global configuration mode.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 11	**show ipv6 mobile host groups** *profile-name*] **Example:** `Router# show ipv6 mobile host groups`	Displays information about Mobile IPv6 host groups.

Configuration Examples for Mobile IPv6 High Availability

Example Configuring Host Groups for Mobile IPv6

The following example shows how to configure a Mobile IPv6 host group named group1:

```
ipv6 mobile host group group1

  nai sri@cisco.com

  address autoconfig

  authentication spi 500 key ascii cisco
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

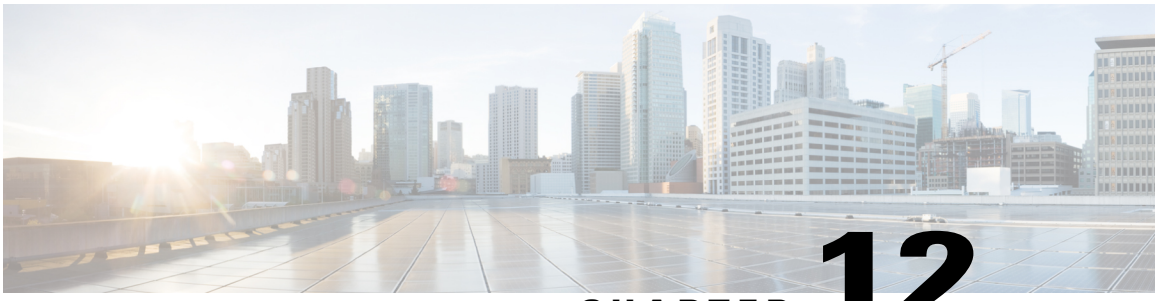
Feature Information for Mobile IPv6 High Availability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 4: Feature Information for Mobile IPv6 High Availability

Feature Name	Releases	Feature Information
Mobile IPv6 High Availability	12.4(11)T	This phase of development for Mobile IPv6 includes support for NAI, alternate authentication, and native IPv6 tunnel infrastructure. The following commands were introduced or modified: **address**, **authentication**, **binding**, **host group**, **ipv6 mobile home-agent**, **nai**, **show ipv6 mobile host groups**, **show ipv6 mobile tunnels**.



CHAPTER 12

IPv6 ACL Extensions for Mobile IPv6

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users, whether they are within their enterprise networks or away from home.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 ACL Extensions for Mobile IPv6

Mobile IPv6 Overview

Mobile IPv4 provides an IPv4 node with the ability to retain the same IPv4 address and maintain uninterrupted network and application connectivity while traveling across networks. In Mobile IPv6, the IPv6 address space enables Mobile IP deployment in any kind of large environment. No foreign agent is needed to use Mobile IPv6.

System infrastructures do not need an upgrade to accept Mobile IPv6 nodes. IPv6 autoconfiguration simplifies mobile node (MN) Care of Address (CoA) assignment.

Mobile IPv6 benefits from the IPv6 protocol itself; for example, Mobile IPv6 uses IPv6 option headers (routing, destination, and mobility) and benefits from the use of neighbor discovery.

Mobile IPv6 provides optimized routing, which helps avoid triangular routing. Mobile IPv6 nodes work transparently even with nodes that do not support mobility (although these nodes do not have route optimization).

Mobile IPv6 is fully backward-compatible with existing IPv6 specifications. Therefore, any existing host that does not understand the new mobile messages will send an error message, and communications with the mobile node will be able to continue, albeit without the direct routing optimization.

How Mobile IPv6 Works

To implement Mobile IPv6, you need a home agent on the home subnet on which the mobile node's home address resides. The IPv6 home address (HA) is assigned to the mobile node. The mobile node obtains a new IPv6 address (the CoA) on networks to which it connects. The home agent accepts BUs from the mobile node informing the agent of the mobile node's location. The home agent then acts as proxy for the mobile node, intercepting traffic to the mobile node's home address and tunneling it to the mobile node.

The mobile node informs a home agent on its original home network about its new address, and the correspondent node communicates with the mobile node about the CoA. Because of the use of ingress filtering, the mobile node reverses tunnel return traffic to the home agent, so that the mobile node source address (that is, its home address) will always be topographically correct.

Mobile IPv6 is the ability of a mobile node to bypass the home agent when sending IP packets to a correspondent node. Optional extensions make direct routing possible in Mobile IPv6, though the extensions might not be implemented in all deployments of Mobile IPv6.

Direct routing is built into Mobile IPv6, and the direct routing function uses the IPv6 routing header and the IPv6 destination options header. The routing header is used for sending packets to the mobile node using its current CoA, and the new home address destination option is used to include the mobile node's home address, because the current CoA is the source address of the packet.

Packet Headers in Mobile IPv6

The basic IPv6 packet header has 8 fields with a total size of 40 octets (320 bits). Fields were removed from the IPv6 header compared with the IPv4 header because, in IPv6, fragmentation is not handled by routers and checksums at the network layer are not used. Instead, fragmentation in IPv6 is handled by the source of a

packet and checksums at the data link layer and transport layer are used. Additionally, the basic IPv6 packet header and options field are aligned to 64 bits, which can facilitate the processing of IPv6 packets.

Mobile IPv6 uses the routing and destination option headers for communications between the mobile node and the correspondent node. The new mobility option header is used only for the BU process.

Several ICMP message types have been defined to support Mobile IPv6. IPv6 access lists can be configured to allow IPv6 access list entries matching Mobile-IPv6-specific ICMP messages to be configured and to allow the definition of entries to match packets containing Mobile IPv6 extension headers.

For further information on IPv6 packet headers, refer to the "Implementing IPv6 Addressing and Basic Connectivity" module.

How to Configure IPv6 ACL Extensions for Mobile IPv6

Enabling Mobile IPv6 on the Router

You can customize interface configuration parameters before you start Mobile IPv6 (see the Customizing Mobile IPv6 on the Interface, on page 161) or while Mobile IPv6 is in operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile home-agent** [**preference** *preference-value*
5. **exit**
6. **exit**
7. **show ipv6 mobile globals**
8. **show ipv6 mobile home-agent** *interface-type interface-number* [*prefix*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 mobile home-agent** [**preference** *preference-value* **Example:** `Router(config-if)# ipv6 mobile home-agent`	Initializes and starts the Mobile IPv6 home agent on a specific interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 7	**show ipv6 mobile globals** **Example:** `Router# show ipv6 mobile globals`	Displays global Mobile IPv6 parameters.
Step 8	**show ipv6 mobile home-agent** *interface-type interface-number* [*prefix*]] **Example:** `Router# show ipv6 mobile home-agent`	Displays local and discovered neighboring home agents.

Filtering Mobile IPv6 Protocol Headers and Options

IPv6 extension headers have been developed to support the use of option headers specific to Mobile IPv6. The IPv6 mobility header, the type 2 routing header, and the destination option header allow the configuration of IPv6 access list entries that match Mobile-IPv6-specific ICMPv6 messages and allow the definition of entries to match packets that contain the new and modified IPv6 extension headers. For more information on how to create, configure, and apply IPv6 access lists, refer to the implementing Traffic Filters and Firewalls for IPv6 Security module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit icmp** {*source-ipv6-prefix* / *prefix-length* | **any** | **host** *source-ipv6-address*| **auth**} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list list1`	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.

Step 4	**permit icmp** {*source-ipv6-prefix* / *prefix-length*	**any**	**host** *source-ipv6-address*| **auth**} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length*	**any**	**host** *destination-ipv6-address*	**auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]	*icmp-message*] [**dest-option-type** [*doh-number*	*doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number*	*mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
									
									Example:
									`Router(config-ipv6-acl)# permit icmp host 2001:DB8:0:4::32 any routing-type 2`
										Specifies permit or deny conditions for Mobile-IPv6-specific option headers in an IPv6 access list.
										• The *icmp-type* argument can be (but is not limited to) one of the following Mobile-IPv6-specific options:
										  • dhaad-request—numeric value is 144
										  • dhaad-reply—numeric value is 145
										  • mpd-solicitation—numeric value is 146
										  • mpd-advertisement—numeric value is 147
										• When the **dest-option-type** keyword with the *doh-number* or *doh-type* argument is used, IPv6 packets are matched against the destination option extension header within each IPv6 packet header.

	Command or Action	Purpose
	Example: `Router(config-ipv6-acl)# deny icmp host 2001:DB8:0:4::32 any routing-type 2`	• When the **mobility** keyword is used, IPv6 packets are matched against the mobility extension header within each IPv6 packet header. • When the **mobility-type** keyword with the *mh-number* or *mh-type* argument is used, IPv6 packets are matched against the mobility-type option extension header within each IPv6 packet header. • When the **routing-type** keyword and *routing-number* argument are used, IPv6 packets are matched against the routing-type option extension header within each IPv6 packet header.

Controlling ICMP Unreachable Messages

When IPv6 is unable to route a packet, it generates an appropriate ICMP unreachable message directed toward the source of the packet. Perform this task to control ICMP unreachable messages for any packets arriving on a specified interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 unreachables**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**ipv6 unreachables** **Example:** `Router(config-if)# ipv6 unreachables`	Enables the generation of ICMPv6 unreachable messages for any packets arriving on the specified interface.

Configuration Examples for IPv6 ACL Extensions for Mobile IPv6

Example: Viewing IPv6 Mobile Information on an Interface

```
Device(config-if)# ipv6 nd ra-interval 100 60
Subsequent use of the show ipv6 interface then displays the interval as follows:

Router(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

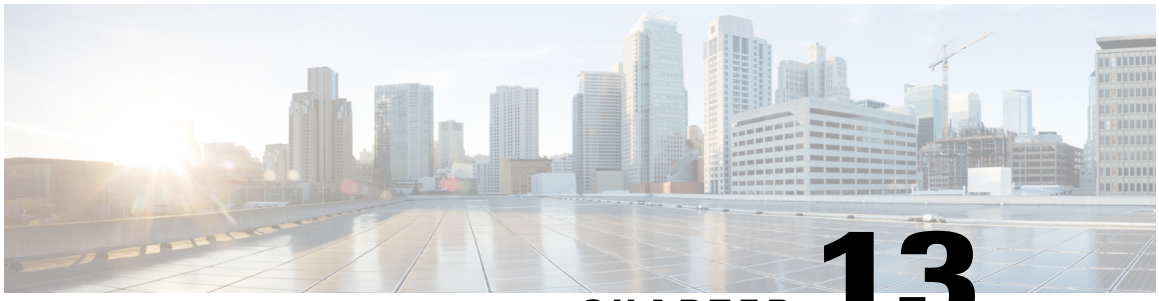
Feature Information for IPv6 ACL Extensions for Mobile IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 5: Feature Information for IPv6 ACL Extensions for Mobile IPv6

Feature Name	Releases	Feature Information
IPv6 ACL Extensions for Mobile IPv6	12.4(2)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S 15.0(1)SY	IPv6 access lists can be configured to allow IPv6 access list entries matching Mobile-IPv6-specific ICMP messages to be configured and to allow the definition of entries to match packets containing Mobile IPv6 extension headers. The following commands were introduced or modified: **deny**, **ipv6 access-list**, **ipv6 unreachables**, **permit**.



CHAPTER 13

Mobile IPv6 Home Agent

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users, whether they are within their enterprise networks or away from home.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Mobile IPv6 Home Agent

Mobile IPv6 Overview

Mobile IPv4 provides an IPv4 node with the ability to retain the same IPv4 address and maintain uninterrupted network and application connectivity while traveling across networks. In Mobile IPv6, the IPv6 address space enables Mobile IP deployment in any kind of large environment. No foreign agent is needed to use Mobile IPv6.

System infrastructures do not need an upgrade to accept Mobile IPv6 nodes. IPv6 autoconfiguration simplifies mobile node (MN) Care of Address (CoA) assignment.

Mobile IPv6 benefits from the IPv6 protocol itself; for example, Mobile IPv6 uses IPv6 option headers (routing, destination, and mobility) and benefits from the use of neighbor discovery.

Mobile IPv6 provides optimized routing, which helps avoid triangular routing. Mobile IPv6 nodes work transparently even with nodes that do not support mobility (although these nodes do not have route optimization).

Mobile IPv6 is fully backward-compatible with existing IPv6 specifications. Therefore, any existing host that does not understand the new mobile messages will send an error message, and communications with the mobile node will be able to continue, albeit without the direct routing optimization.

How Mobile IPv6 Works

To implement Mobile IPv6, you need a home agent on the home subnet on which the mobile node's home address resides. The IPv6 home address (HA) is assigned to the mobile node. The mobile node obtains a new IPv6 address (the CoA) on networks to which it connects. The home agent accepts BUs from the mobile node informing the agent of the mobile node's location. The home agent then acts as proxy for the mobile node, intercepting traffic to the mobile node's home address and tunneling it to the mobile node.

The mobile node informs a home agent on its original home network about its new address, and the correspondent node communicates with the mobile node about the CoA. Because of the use of ingress filtering, the mobile node reverses tunnel return traffic to the home agent, so that the mobile node source address (that is, its home address) will always be topographically correct.

Mobile IPv6 is the ability of a mobile node to bypass the home agent when sending IP packets to a correspondent node. Optional extensions make direct routing possible in Mobile IPv6, though the extensions might not be implemented in all deployments of Mobile IPv6.

Direct routing is built into Mobile IPv6, and the direct routing function uses the IPv6 routing header and the IPv6 destination options header. The routing header is used for sending packets to the mobile node using its current CoA, and the new home address destination option is used to include the mobile node's home address, because the current CoA is the source address of the packet.

Mobile IPv6 Home Agent

The home agent is one of three key components in Mobile IPv6. The home agent works with the correspondent node and mobile node to enable Mobile IPv6 functionality:

- Home agent--The home agent maintains an association between the mobile mode's home IPv4 or IPv6 address and its CoA (loaned address) on the foreign network.
- Correspondent node--The correspondent node is the destination IPv4 or IPv6 host in session with a mobile node.
- Mobile node--An IPv4 or IPv6 host that maintains network connectivity using its home IPv4 or IPv6 address, regardless of the link (or network) to which it is connected.

The following sections describe Mobile IPv6 home agent functionality:

Binding Cache in Mobile IPv6 Home Agent

A separate binding cache is maintained by each IPv6 node for each of its IPv6 addresses. When the router sends a packet, it searches the binding cache for an IPv6 address before it searches the neighbor discovery conceptual destination cache.

The binding cache for any one of a node's IPv6 addresses may contain one entry for each mobile node home address. The contents of all of a node's binding cache entries are cleared when it reboots.

Binding cache entries are marked either as home registration or correspondent registration entries. A home registration entry is deleted when its binding lifetime expires; other entries may be replaced at any time through a local cache replacement policy.

Binding Update List in Mobile IPv6 Home Agent

A binding update (BU) list is maintained by each mobile node. The BU list records information for each BU sent by this mobile node whose lifetime has not yet expired. The BU list includes all BUs sent by the mobile node--those bindings sent to correspondent nodes, and those bindings sent to the mobile node's home agent.

The mobility extension header has a new routing header type and a new destination option, and it is used during the BU process. This header is used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings.

Home Agents List

A home agents list is maintained by each home agent and each mobile node. The home agents list records information about each home agent from which this node has recently received a router advertisement in which the home agent (H) bit is set.

Each home agent maintains a separate home agents list for each link on which it is serving as a home agent. This list is used by a home agent in the dynamic home agent address discovery mechanism. Each roaming mobile node also maintains a home agents list that enables it to notify a home agent on its previous link when it moves to a new link.

IPv6 Neighbor Discovery with Mobile IPv6

The IPv6 neighbor discovery feature has the following modifications to allow the feature to work with Mobile IPv6:

- Modified router advertisement message format--has a single flag bit that indicates home agent service

- Modified prefix information option format--allows a router to advertise its global address
- New advertisement interval option format
- New home agent information option format
- Changes to sending router advertisements
- Provide timely movement detection for mobile nodes

How to Configure Mobile IPv6 Home Agent

Enabling Mobile IPv6 on the Router

You can customize interface configuration parameters before you start Mobile IPv6 (see the Customizing Mobile IPv6 on the Interface, on page 161) or while Mobile IPv6 is in operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile home-agent** [**preference** *preference-value*
5. **exit**
6. **exit**
7. **show ipv6 mobile globals**
8. **show ipv6 mobile home-agent** *interface-type interface-number* [*prefix*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 mobile home-agent** [**preference** *preference-value* **Example:** `Router(config-if)# ipv6 mobile home-agent`	Initializes and starts the Mobile IPv6 home agent on a specific interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 7	**show ipv6 mobile globals** **Example:** `Router# show ipv6 mobile globals`	Displays global Mobile IPv6 parameters.
Step 8	**show ipv6 mobile home-agent** *interface-type interface-number* [*prefix*]] **Example:** `Router# show ipv6 mobile home-agent`	Displays local and discovered neighboring home agents.

Configuring Binding Information for Mobile IPv6

Before you start Mobile IPv6 on a specified interface, you can configure binding information on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile home-agent**
4. **binding access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*
5. **exit**
6. **exit**
7. **show ipv6 mobile binding** [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*
8. **show ipv6 mobile traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mobile home-agent** **Example:** `Router(config)# ipv6 mobile home-agent`	Places the router in home-agent configuration mode.
Step 4	**binding access** *access-list-name*	*auth-option*	*seconds*	*maximum*	*refresh* **Example:** `Router(config-ha)# binding`	Configures binding options for the Mobile IPv6 home agent feature.
Step 5	**exit** **Example:** `Router(config-ha)# exit`	Exits home-agent configuration mode, and returns the router to global configuration mode.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 7	**show ipv6 mobile binding** [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number* **Example:** `Router# show ipv6 mobile binding`	Displays information about the binding cache.
Step 8	**show ipv6 mobile traffic** **Example:** `Router# show ipv6 mobile traffic`	Displays information about BUs received and BAs sent.

Customizing Mobile IPv6 on the Interface

Perform this task to customize interface configuration parameters for your router configuration. You can set these interface configuration parameters before you start Mobile IPv6 or while Mobile IPv6 is in operation. You can customize any of these parameters, as desired.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile home-agent** [**preference** *preference-value*
5. **ipv6 nd advertisement-interval**
6. **ipv6 nd prefix** {*ipv6-prefix / prefix-length* | **default**} [[*valid-lifetime preferred-lifetime* | **at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-rtr-address** | **no-autoconfig**
7. **ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | **msec** *maximum-msecs* [*minimum-msecs*]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 3`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 mobile home-agent** [**preference** *preference-value* **Example:** `Router(config-if)# ipv6 mobile home-agent preference 10`	Configures the Mobile IPv6 home agent preference value on the interface.
Step 5	**ipv6 nd advertisement-interval** **Example:** `Router(config-if)# ipv6 nd advertisement-interval`	Configures the advertisement interval option to be sent in RAs.
Step 6	**ipv6 nd prefix** {*ipv6-prefix* / *prefix-length* | **default**} [[*valid-lifetime preferred-lifetime* | **at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-rtr-address** | **no-autoconfig** **Example:** `Router(config-if)# ipv6 nd prefix 2001:DB8::/35 1000 900`	Configures which IPv6 prefixes are included in IPv6 RAs.
Step 7	**ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | **msec** *maximum-msecs* [*minimum-msecs*]} **Example:** `Router(config-if)# ipv6 nd ra interval 201`	Configures the interval between IPv6 RA transmissions on an interface.

Configuration Examples for Mobile IPv6 Home Agent

Example Enabling Mobile IPv6 on the Router

The following example shows how to configure and enable Mobile IPv6 on a specified interface:

```
Router> enable
Router# config terminal
Router(config)# interface Ethernet 1
Router(config-if)# ipv6 mobile home-agent
```

Example: Viewing IPv6 Mobile Information on an Interface

```
Device(config-if)# ipv6 nd ra-interval 100 60
Subsequent use of the show ipv6 interface then displays the interval as follows:

Router(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*

Related Topic	Document Title
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

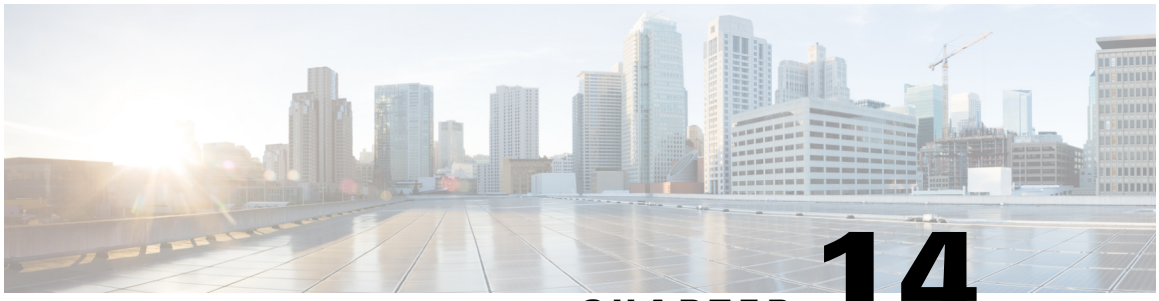
Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Mobile IPv6 Home Agent

Table 6: Feature Information for Mobile IPv6 Home Agent

Feature Name	Releases	Feature Information
Mobile IPv6 Home Agent	12.3(4)T	The Mobile IPv6 feature uses the IPv6 address space to enable Mobile IP deployment in any kind of large environment. No foreign agent is needed to use Mobile IPv6. The following commands were introduced or modified: **binding access**, **ipv6 mobile home-agent**, **ipv6 nd advertisement-interval**, **ipv6 nd prefix**, **ipv6 nd ra interval**, **show ipv6 mobile globals**, **show ipv6 mobile home-agent**.



CHAPTER 14

IPv6 NEMO

The network mobility (NEMO) basic support protocol enables mobile IPv6 networks to attach to different points in the Internet. This protocol is an extension of Mobile IPv6 and allows session continuity for every node in the mobile network as the network moves.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 NEMO

When using the network mobility (NEMO) basic support protocol feature, users should not enable any IPv6 routing protocols on any of the roaming interfaces.

Information About IPv6 NEMO

IPv6 NEMO

The NEMO basic support protocol enables mobile IPv6 networks to attach to different points in the Internet. This protocol is an extension of Mobile IPv6 and allows session continuity for every node in the mobile network as the network moves. NEMO also allows every node in the mobile network to be reachable while the user is moving. The mobile router, which connects the network to the Internet, runs the NEMO basic support protocol with its home agent (HA). NEMO allows network mobility to be transparent to the nodes inside the mobile network.

The NEMO router maintains a mobile route, which is the default route for IPv6 over the roaming interface.

NEMO-Compliant Home Agent

Protocol extensions to Mobile IPv6 are used to enable support for network mobility. The extensions are backward-compatible with existing Mobile IPv6 functionality. A NEMO-compliant home agent can operate as a Mobile IPv6 home agent.

The dynamic home agent address discovery (DHAAD) mechanism allows a mobile node to discover the address of the home agent on its home link. The following list describes DHAAD functionality and features:

- The mobile router sends Internet Control Message Protocol (ICMP) home agent address discovery requests to the Mobile IPv6 home agent's anycast address for the home subnet prefix.
- A new flag (R) is introduced in the DHAAD request message, indicating the desire to discover home agents that support mobile routers. This flag is added to the DHAAD reply message as well.
- On receiving the home agent address discovery reply message, the mobile router discovers the home agents operating on the home link.
- The mobile router attempts home registration to each of the home agents until its registration is accepted. The mobile router waits for the recommended length of time between its home registration attempts with each of its home registration attempts.

Implicit Prefix Registration

When using implicit prefix registration, the mobile router does not register any prefixes as part of the binding update with its home agent. This function requires a static configuration at the home agent, and the home agent must have the information of the associated prefixes with the given mobile router for it to set up route forwarding.

Explicit Prefix Registration

When using explicit prefix registration, the mobile router presents a list of prefixes to the home agent as part of the binding update procedure. If the home agent determines that the mobile router is authorized to use these prefixes, it sends a bind acknowledgment message.

IPv6 Neighbor Discovery Duplicate Address Detection in NEMO

IPv6 routers are required to run duplicate address detection (DAD) on all IPv6 addresses obtained in stateless and stateful autoconfiguration modes before assigning them to any of its interfaces. Whenever an mobile router roams and obtains an IPv6 address, the mobile router must perform DAD on the newly obtained care-of address and on its link-local address in order to avoid address collisions.

However, the DAD feature adds significant handoff delays in certain Layer 2 environments. These delays may be avoided by using optimistic DAD techniques. NEMO supports optimization options for omitting DAD on care-of address or on both the care-of address and link-local address.

For further information on IPv6 neighbor discovery, refer to the *Implementing IPv6 Addressing and Basic Connectivity* module.

How to Enable IPv6 NEMO

Enabling and Configuring NEMO on the IPv6 Mobile Router

The NEMO basic support protocol enables mobile IPv6 networks to attach to different points in the Internet.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile router**
4. **eui-interface** *interface-type interface-number*
5. **home-network** *ipv6-prefix*
6. **home-address** {**home-network** | *ipv6-address-identifier* | *interface*
7. **explicit-prefix**
8. **register** {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}
9. **exit**
10. **exit**
11. **show ipv6 mobile router running-config** | **status**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mobile router** **Example:** `Router(config)# ipv6 mobile router`	Enables IPv6 NEMO functionality on a router, and places the router in IPv6 mobile router configuration mode.
Step 4	**eui-interface** *interface-type interface-number* **Example:** `Router(IPv6-mobile-router)# eui-interface Ethernet0/0`	Uses the Media Access Control (MAC) address from a specified interface for deriving the IPv6 mobile home address.
Step 5	**home-network** *ipv6-prefix* **Example:** `Router(IPv6-mobile-router)# home-network 2001:0DB1:1/64`	Specifies the home network's IPv6 prefix on the mobile router. • Users can configure up to 10 home-network entries, and they are used in order of priority. The prefix identifies the home network of the mobile router and is used to discover when the mobile router is at home.
Step 6	**home-address** {**home-network** | *ipv6-address-identifier* | *interface* **Example:** `Router(IPv6-mobile-router)# home-address home-network eui-64`	Specifies the mobile router home address using an IPv6 address or interface identifier. • When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.
Step 7	**explicit-prefix** **Example:** `Router(IPv6-mobile-router)# explicit-prefix`	Registers IPv6 prefixes connected to the IPv6 mobile router.
Step 8	**register** {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*} **Example:** `Router(IPv6-mobile-router)# register lifetime 600`	Controls the registration parameters of the IPv6 mobile router.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(IPv6-mobile-router)# exit`	Exits IPv6 mobile router configuration mode, and returns the router to global configuration mode.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 11	**show ipv6 mobile router running-config** | **status**] **Example:** `Router# show ipv6 mobile router`	Displays configuration information and monitoring statistics about the IPv6 mobile router.

Enabling NEMO on the IPv6 Mobile Router Home Agent

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router nemo**
4. **distance** [*mobile-distance*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 router nemo** **Example:** `Router(config)# ipv6 router nemo`	Enables the NEMO routing process on the home agent and place the router in router configuration mode.
Step 4	**distance** [*mobile-distance*] **Example:** `Router(config-rtr)# distance 10`	Defines an administrative distance for NEMO routes.

Enabling Roaming on the IPv6 Mobile Router Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile router-service roam** [**bandwidth-efficient** | **cost-efficient** | **priority** *value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**ipv6 mobile router-service roam** [**bandwidth-efficient** | **cost-efficient** | **priority** *value*]	Enables the IPv6 mobile router interface to roam.

	Command or Action	Purpose
	Example: `Router(config-if)# ipv6 mobile router-service roam`	

Configuration Examples for IPv6 NEMO

Example Enabling and Configuring NEMO on the IPv6 Mobile Router

The following example shows how to enable and configure NEMO on the IPv6 mobile router. The /128 subnet must be used; otherwise, the IPv6 mobile router will fail to register because it will believe the home network is locally connected:

```
ipv6 unicast-routing
!
interface ethernet0/0
no ip address
ipv6 address 2001:DB8:2000::1111/128
ipv6 nd ra mtu suppress
!
interface ethernet0/1
no ip address
ipv6 address 2001:DB8:1000::1111/128
ipv6 nd ra mtu suppress
!
interface Ethernet0/0
description Roaming Interface to AR2
no ip address
ipv6 address autoconfig
ipv6 enable
ipv6 nd ns-interval 5000
ipv6 mobile router-service roam
ipv6 rip home enable
!
interface Ethernet0/1
description Mobile Network Interface
no ip address
ipv6 address 2001:DB8:8000::8001/64
ipv6 enable
ipv6 nd advertisement-interval
ipv6 nd ra interval msec 1000
ipv6 rip home enable
!
interface Ethernet1/1
description Roaming Interface to AR1
no ip address
ipv6 address autoconfig
ipv6 enable
ipv6 nd ns-interval 5000
ipv6 mobile router-service roam priority 99
ipv6 rip home enable
!
ipv6 router rip home
!
ipv6 mobile router
```

```
host group mr-host-group
nai mr1@cisco.com
address 2001:DB8:2000::1112/128
authentication spi hex 100 key ascii hi
exit
home-network 2001:DB8:2000::/64 discover priority 127
home-network 2001:DB8:1000::/64 discover
home-address home-network eui-64
explicit-prefix
register lifetime 60
register retransmit initial 1000 maximum 1000 retry 1
register extend expire 20 retry 1 interval 1
```

Example Enabling NEMO on the IPv6 Mobile Router Home Agent

The following example shows how to enable and configure NEMO on the IPv6 mobile router home agent. The anycast address is needed for DHAAD to work. The **redistribute nemo** command redistributes NEMO routes into the routing protocol:

```
ipv6 unicast-routing
!
interface Ethernet0/2
description To Network
no ip address
no ipv6 address
ipv6 address 2001:DB8:2000::2001/64
ipv6 address 2001:DB8:2000::FDFF:FFFF:FFFF:FFFE/64 anycast
ipv6 enable
ipv6 nd advertisement-interval
ipv6 nd ra lifetime 2
ipv6 nd ra interval msec 1000
ipv6 mobile home-agent preference 100
ipv6 mobile home-agent
ipv6 rip home enable
!
interface Ethernet2/2
description To CN2
no ip address
no ipv6 address
ipv6 address 2001:DB8:3000::3001/64
ipv6 enable
ipv6 rip home enable
!
ipv6 router nemo
!
ipv6 router rip home
redistribute nemo
poison-reverse
!
ipv6 mobile home-agent
host group mr-host-group
nai mr1@cisco.com
address 2001:DB8:2000::1112/64
authentication spi hex 100 key ascii hi
exit
host group mr2-host-group
nai mr2@cisco.com
address 2001:DB8:2000::2222
authentication spi decimal 512 key hex 12345678123456781234567812345678
exit
```

Example Enabling Roaming on the IPv6 Mobile Router Interface

The following example shows how to enable roaming on the IPv6 mobile router interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 mobile router-service roam
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 NEMO

Table 7: Feature Information for IPv6 NEMO

Feature Name	Releases	Feature Information
Mobile IP - Mobile Networks v6 - Basic NEMO	12.4(20)T	The NEMO basic support protocol enables mobile IPv6 networks to attach to different points in the Internet. The following commands were introduced or modified: **distance**, **eui-interface**, **explicit-prefix**, **home-address**, **home-network**, **ipv6 mobile router**, **ipv6 mobile router-service roam**, **ipv6 router nemo**, **register**, **show ipv6 mobile router**.

INDEX

R

S