Cisco IOS IP Mobility Configuration Guide

Release 12.2SR

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

About Cisco IOS Software Documentation

Last Updated: November 20, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the **^** symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

- Cisco IOS Documentation Set, page iv
- Cisco IOS Documentation on Cisco.com, page iv
- Configuration Guides, Command References, and Supplementary Resources, page v

Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

http://www.cisco.com/go/techdocs

Table 1 Cisco IOS Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS AppleTalk Configuration Guide* • *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
• *Cisco IOS Asynchronous Transfer Mode Configuration Guide* • *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging Command Reference* • *Cisco IOS IBM Networking Command Reference*	Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
• *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
• *Cisco IOS DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.
• *Cisco IOS High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
• *Cisco IOS Integrated Session Border Controller Command Reference*	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS IP Mobility Configuration Guide* • *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
• *Cisco IOS IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
• *Cisco IOS IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
• *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide* • *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
• *Cisco IOS Mobile Wireless Home Agent Configuration Guide* • *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
• *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide* • *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
• *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide* • *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.
• *Cisco IOS Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS Multi-Topology Routing Configuration Guide* • *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• *Cisco IOS NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
• *Cisco IOS Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
• *Cisco IOS Optimized Edge Routing Configuration Guide* • *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
• *Cisco IOS Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS Service Selection Gateway Configuration Guide* • *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
• *Cisco IOS Software Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *Cisco IOS Software Modularity Installation and Configuration Guide* • *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• *Cisco IOS Virtual Switch Command Reference*	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• *Cisco IOS VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
• *Cisco IOS Wireless LAN Configuration Guide* • *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS System Message Guide	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator.
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product/Technologies Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes the purpose of the CLI interactive Help commands.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

```
Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

partial command?

```
Router(config)# zo?
zone  zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command ?

```
Router(config-if)# pppoe ?
  enable         Enable pppoe
  max-sessions   Maximum PPPOE sessions
```

command keyword ?

```
Router(config-if)# pppoe enable ?
  group   attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>

Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a numeral. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

  Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following document:

- *Cisco IOS Release 12.4T System Message Guide*

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

- Cisco Product/Technology Support

  http://www.cisco.com/go/techdocs

- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html

- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)

  http://www.cisco.com/kobayashi/sw-center/

- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl

---

Mobile IP

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.

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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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.

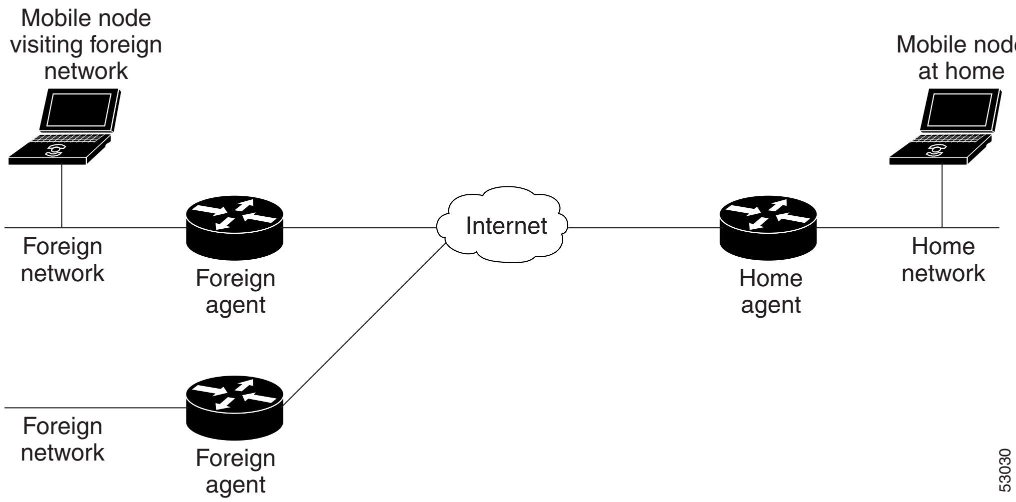
Mobile IP is scalable for the Internet because it is based on IP—any media that supports IP can support Mobile IP. Mobile IP does not drop the network prefix of the IP address of the node, which is critical to the proper routing of packets throughout the Internet. Also, certain network services, such 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 Figure 1:

- 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
- Registration
- Routing

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.

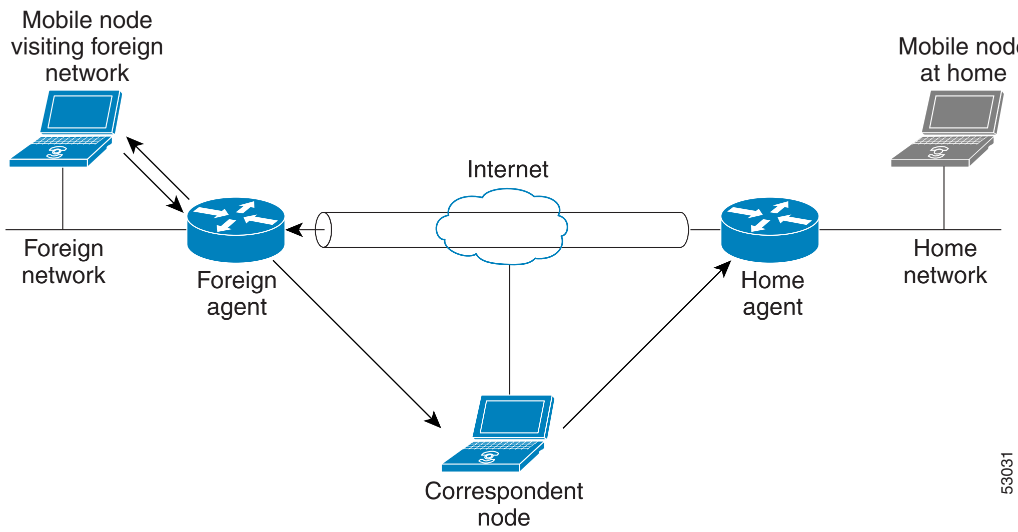
Routing

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 Figure 2 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" 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" 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" section later in this chapter for more information on HA-HA authentication.

Storing Security Associations

As discussed in the "Mobile IP Security" 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:

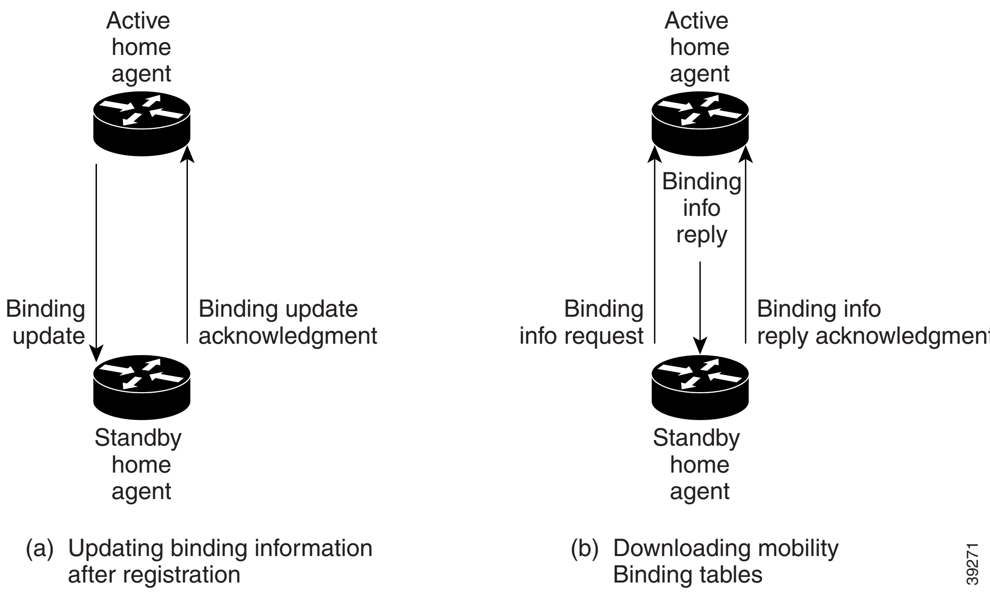
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN
- An MN that requires the HA interface to be on the same subnet as the MN, that is, the HA and the MN must be on the same home network

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 Figure 3 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 Figure 3 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 (Required)
- Enabling Foreign Agent Services (Required)
- Configuring AAA in the Mobile IP Environment (Optional)
- Configuring RADIUS in the Mobile IP Environment (Optional)
- Configuring TACACS+ in the Mobile IP Environment (Optional)
- Verifying Setup (Optional)
- Monitoring and Maintaining Mobile IP (Optional)
- Shutting Down Mobile IP (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:

	Command	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.

	Command	Purpose
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:

	Command	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:

	Command	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:

	Command	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:

	Command	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.[1]
Router# **debug ip mobile host**	Displays mobility events.

1. 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:

	Command	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

To configure your routers for Mobile IP HA redundancy, perform the required tasks described in the following sections:

- Enabling Mobile IP (Required)

- Enabling HSRP (Required)
- Enabling HA Redundancy for a Physical Network (Required)

Depending on your network configuration, perform one of the optional tasks described in the following sections:

- Enabling HA Redundancy for a Physical Network (Optional)
- Enabling HA Redundancy for a Virtual Network Using One Physical Network (Optional)
- Enabling HA Redundancy for a Virtual Network Using Multiple Physical Networks (Optional)
- Enabling HA Redundancy for Multiple Virtual Networks Using One Physical Network (Optional)
- Enabling HA Redundancy for Multiple Virtual Networks Using Multiple Physical Networks (Optional)
- Verifying HA Redundancy (Optional)

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:

	Command	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 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:

	Command	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 address`** *`address`* or `Router(config)#` **`ip mobile home-agent`**	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 network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.

	Command	Purpose
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:

	Command	Purpose
Step 1	Router(config-if)# **standby** [*group-number*] **ip** *ip-address*	Enables 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	Router(config)# **ip mobile home-agent address** *address* or 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 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:

	Command	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	`Router(config)#` **`ip mobile home-agent address`** *`address`* or `Router(config)#` **`ip mobile home-agent`**	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:

	Command	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.

	Command	Purpose
Step 4	`Router(config)#` **`ip mobile home-agent address`** *`address`* or 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.
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:

Step 1 Enter the **show ip mobile globals** EXEC command.

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

This section provides the following Mobile IP configuration examples:

- Home Agent Configuration Example
- Home Agent Using AAA Server Example
- Foreign Agent Configuration Example
- Mobile IP HA Redundancy Configuration Examples
  - HA Redundancy for Physical Networks Example
  - HA Redundancy for a Virtual Network Using One Physical Network Example
  - HA Redundancy for a Virtual Network Using Multiple Physical Networks Example
  - HA Redundancy for Multiple Virtual Networks Using One Physical Network Example
  - HA Redundancy for Multiple Virtual Networks Using Multiple Physical Networks Example

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 73839303313233343536313233343536
ip mobile secure host 11.0.0.2 spi 200 key hex 83930313233343536313233343536373
ip mobile secure host 11.0.0.3 spi 300 key hex 43536373839313233330313233343536
ip mobile secure host 11.0.0.4 spi 100 key hex 23334353631323334353637383930313
ip mobile secure host 11.0.0.5 spi 200 key hex 63738393132333435330313233343536
!
! 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

Table 1 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.

Table 1 Mobile IP HA Redundancy Configuration Overview (continued)

Mobile Node Home Network	Physical Connections	Home Agent Address	Configuration
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**
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.

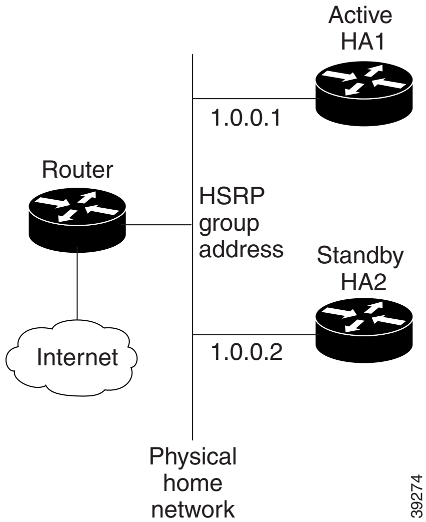
Table 1 Mobile IP HA Redundancy Configuration Overview (continued)

Mobile Node Home Network	Physical Connections	Home Agent Address	Configuration
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**
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

Figure 4 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.

Figure 5 shows an example network topology for the first scenario. Figure 6 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)

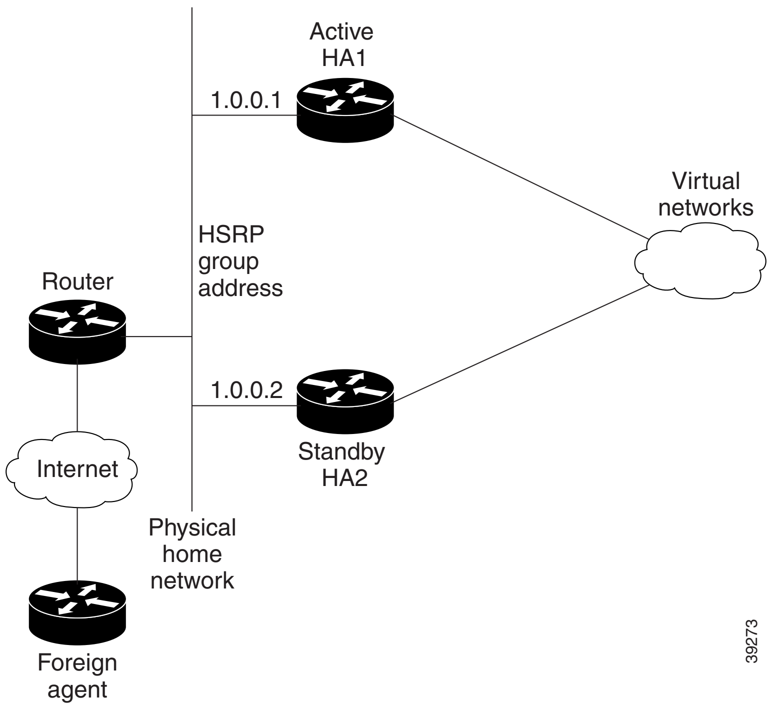
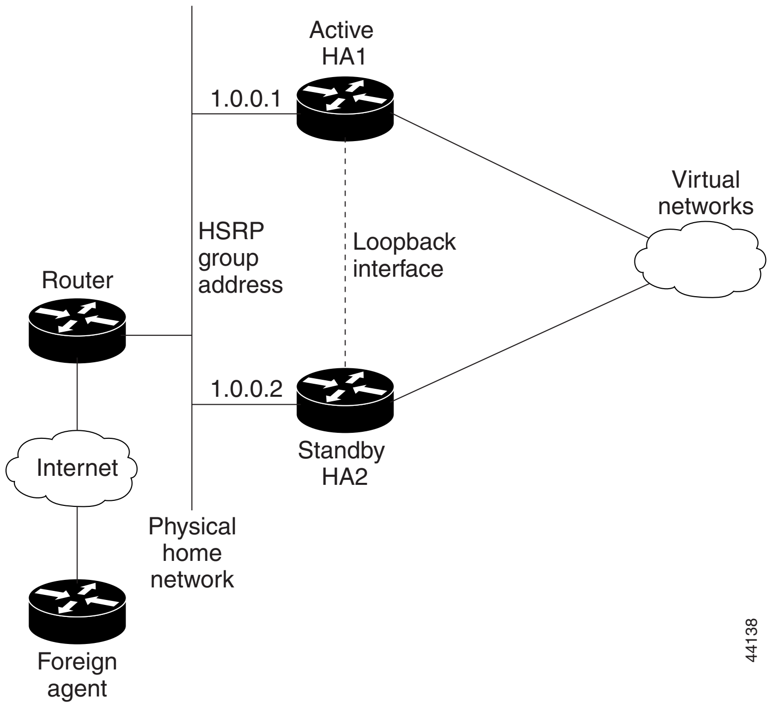


Figure 6 Topology Showing HA Redundancy on Multiple Virtual Networks Using One Physical Network (Same Subnet)



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
```

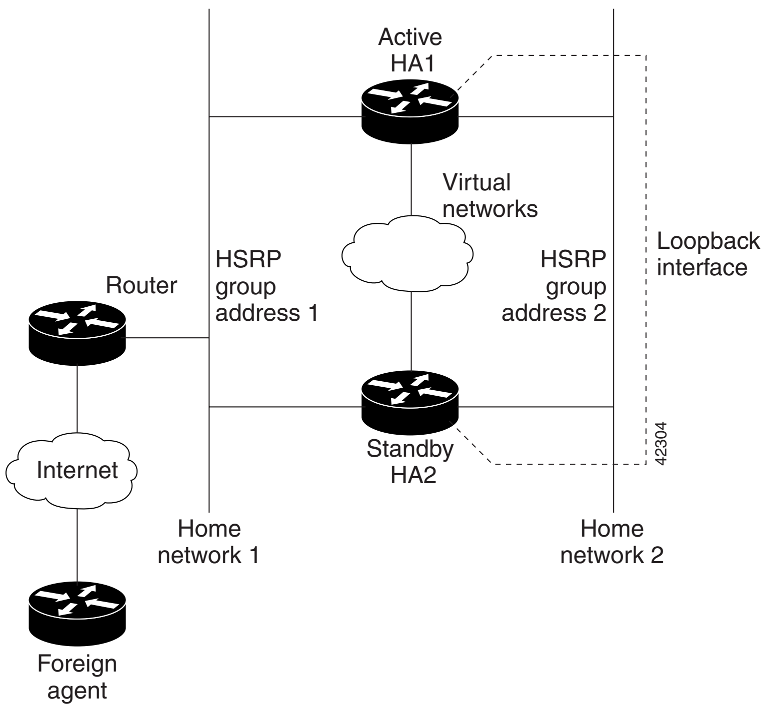
HA Redundancy for Multiple Virtual Networks Using Multiple Physical Networks Example

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.

Figure 7 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
```

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:

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” 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. Table 1 shows the fixed values for objects in the mipSecAssocTable.

Table 1 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

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you want to establish an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

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

See the following sections for configuration tasks for the Mobile IP MIB Support for SNMP feature. Each task in the list is identified as either required or optional:

- Configuring the Router to Send Mobile IP MIB Notifications (required)
- Verifying Mobile IP MIB Configuration (optional)

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:

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.

Note that Mobile IP notifications need not be enabled on a system to process simple Set or Get SNMP requests.

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" 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.

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.	

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

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

This section contains the following procedures:

- Configuring NAT Detect, page 2 (required)
- Verifying the NAT Detect Configuration, page 3 (optional)

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.
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.

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

This section provides the following configuration example:

- Home Agent with NAT Detect Example, page 4

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, page 5
- Standards, page 6
- MIBs, page 6
- RFCs, page 6
- Technical Assistance, page 7

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.

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.	

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

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

This section contains the following procedures:

- Enabling Foreign Agent Reverse Tunneling, page 3 (required)
- Enabling Foreign Agent Reverse Tunneling on the Mobile Router, page 5 (required)
- Verifying Foreign Agent Service Configuration, page 6 (optional)

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	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	**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.

	Command	Purpose
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**] **Example:** `Router(config-if)# 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 as care-of address, lifetime, and service flags to the advertisement.

Enabling Foreign Agent Reverse Tunneling on the Mobile Router

Perform this task to enable foreign agent reverse tunneling on a 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	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	Purpose
Step 3	**`router mobile`** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
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.
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[1]	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

1. 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[1]	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*

1. 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**

Mobile IP—Challenge/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.	

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

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

To configure the Mobile IP—Foreign Agent Challenge/Response feature, you must understand the following concepts:

- Challenge/Response Extensions, page 3

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

This section includes the following procedures:

- Configuring FA Challenge/Response Extensions, page 3
- Verifying Foreign Agent Service Configuration, page 5

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.

Prerequisites

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 forward-mfce**

DETAILED STEPS

	Command	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	Purpose
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* **Example:** `Router(config-if)# ip irdp holdtime 9000`	Length of time in seconds that advertisements are held valid. • 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 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, page 7
- Standards, page 7
- MIBs, page 7
- RFCs, page 8
- Technical Assistance, page 8

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 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[1]	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

1. 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[1]	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*

1. 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**

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.	

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

Information About Generic NAI Support and Home Address Allocation

To following sections describe concepts related to generic NAI support and home address allocation:

- NAI Overview, page 2
- Home Address Allocation, page 3
- Benefits of Generic NAI Support and Home Address Allocation, page 4

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.

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.

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, page 4 (required)
- Configuring AAA in the Mobile IP Environment, page 9 (optional)
- Configuring RADIUS in the Mobile IP Environment, page 10 (optional)
- Verifying Generic NAI Support and Home Address Allocation (optional)

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.

Static IP Addresses

This section describes how to configure the home agent to allocate static IP addresses.

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" 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.

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 user@staticuser.com spi 100 key hex 12345678123456781234567812324 5678`	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.

Dynamic IP Addresses

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

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
5. DHCP pool

Restrictions

- 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*]} **Example:** `Router(config)# ip local pool my-pool 172.21.58.5 172.21.58.250`	(Optional) Configures a local pool of IP addresses.

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 12345678123456781234567812324567`	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" 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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.

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" 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" 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" section for an example.

Output Examples

This section provides the following output examples:

- **Sample Output for the show ip mobile binding Command**
- **Sample Output for the show ip mobile host Command**

- Sample Output for the show ip mobile visitor Command

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

This section provides the following configuration examples:

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
- Standards
- MIBs
- RFCs
- Technical Assistance

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
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[1]	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

1. 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[1]	Title
RFC 2486	*The Network Access Identifier*
RFC 2794	*Mobile IP Network Access Identifier Extension for IPv4*
RFC 3220	*IP Mobility Support for IPv4*

1. 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.

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.	

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

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

The following sections describe concepts related to Mobile IP home agent policy routing:

- Policy Routing, page 2
- Feature Design of Mobile IP Home Agent Policy Routing, page 3

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.

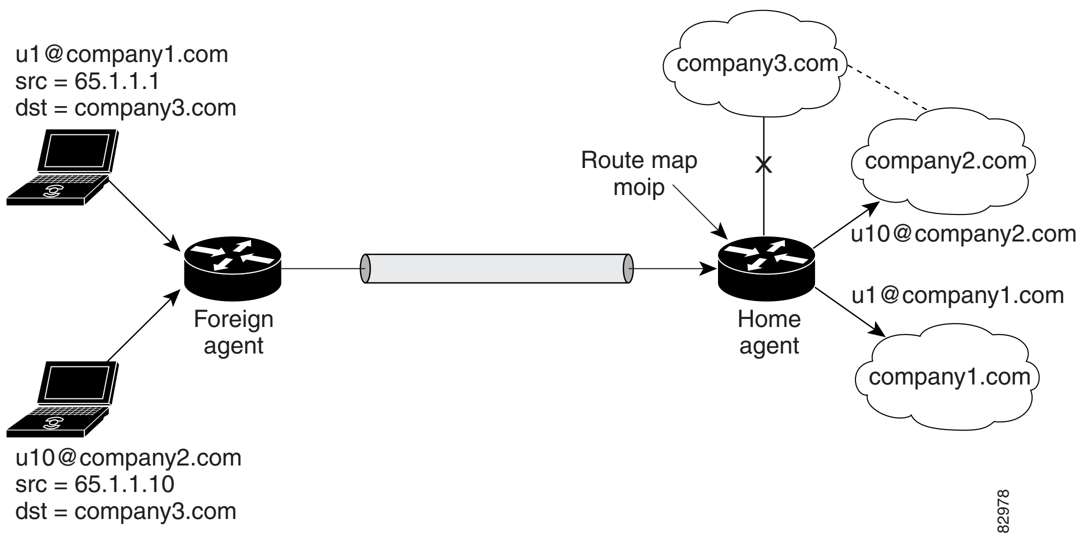
Feature Design of Mobile IP Home Agent Policy Routing

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.

Figure 1 shows a sample topology for home agent policy routing. In Figure 1, 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 1 Sample Topology for Mobile IP Home Agent Policy Routing



How to Configure Mobile IP Home Agent Policy Routing

This section contains the following procedures:

- Enabling Policy Routing on the Home Agent, page 4 (required)
- Defining the Route Map, page 5 (required)
- Verifying Policy Routing on the Home Agent, page 6 (optional)

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.

	Command or Action	Purpose
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.
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.

Restrictions

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** **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	**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 mobile vpn-realm**
6. **show ip policy**

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" 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" 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" 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" 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" section.

Output Examples

This section provides the following output examples:

- **Sample Output for the show ip mobile binding Command**
- **Sample Output for the show ip mobile tunnel Command**
- **Sample Output for the show access-lists Command**
- **Sample Output for the show ip policy Command**
- **Sample Output for the show ip mobile vpn-realm Command**

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

The following section provides a configuration example:

- Home Agent Policy Routing Example, page 9

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, page 10
- Standards, page 10
- MIBs, page 10
- RFCs, page 11
- Technical Assistance

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
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.

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 Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

Before you configure Mobile IP—Home Agent Accounting, you should understand the following concepts:

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.

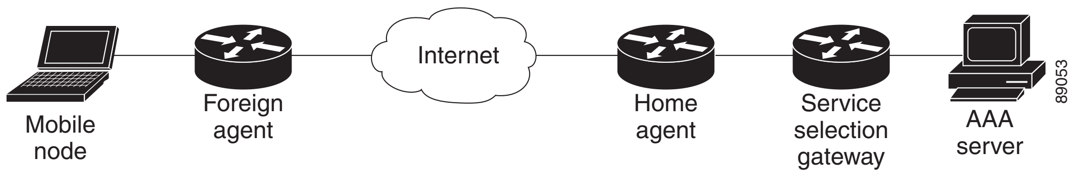
Feature Design of Home Agent Accounting

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 Figure 1.

Figure 1 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 Table 1, including the RADIUS attribute number, which is transparent to the Mobile IP—Home Agent Accounting feature.

Table 1 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

This section contains the following procedures:

- Configuring AAA, page 4 (required)
- Configuring RADIUS, page 5 (required)
- Enabling Home Agent Accounting, page 6 (required)

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.
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** *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. **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*} **Example:** `Router(config)# ip mobile home-agent accounting mylist`	Enables home agent accounting. • 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 12345678123456781234567812324567 8 algorithm md5 mode prefix-suffix`	Specifies the mobility security associations for the mobile host.

	Command or Action	Purpose
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

This section provides the following configuration examples:

- **Home Agent Accounting Example, page 9**

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 12345678123456781234567812324567 8
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, page 9
- Standards, page 10
- MIBs, page 10
- RFCs, page 11
- Technical Assistance, page 11

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

Related Topic	Document Title
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.

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 Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

This section describes the following concepts related to the Mobile IP Dynamic Security Association and Key Distribution feature:

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	*Mobile IP Generic NAI Support and Home Address Allocation* feature document, Release 12.2(13)T
Configuration tasks for Cisco Secure ACS	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.

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 Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

To configure the Mobile IP—Support for RFC 3519 NAT Traversal feature, you should understand the following concepts:

- Design of the Mobile IP—Support for RFC 3519 NAT Traversal Feature, page 2
- Network Address Translation Devices, page 3
- UDP Tunneling, page 3

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.

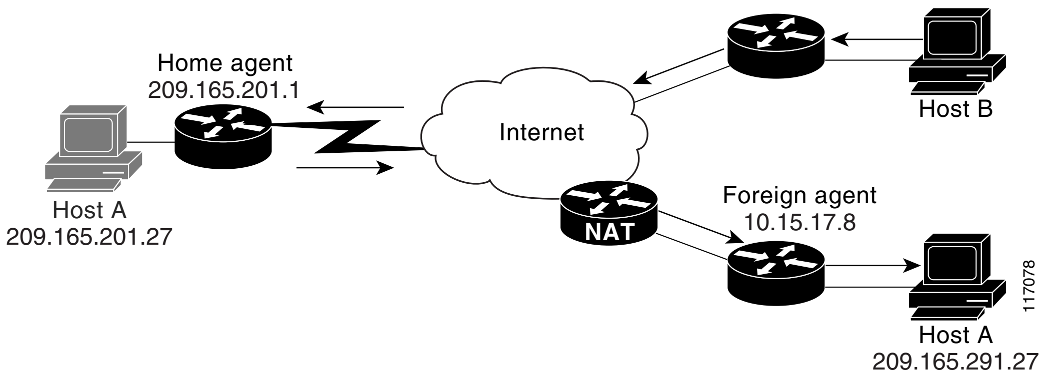
Network Address Translation (NAT) allows for the translation of a private IP address to a public IP address. NAT uses the port number in the second header to organize the translations and determine which translation (if any) to use when it sees a returning packet.

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.

Figure 1 shows Mobile IP components and their relationships.

Figure 1 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

This section contains the following tasks:

- Configuring the Home Agent for NAT Traversal Support, page 5 (required)
- Configuring the Foreign Agent for NAT Traversal Support, page 6 (required)
- Verifying NAT Traversal Support, page 7 (optional)

Configuring the Home Agent for NAT Traversal Support

This task shows you how to configure the HA 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.
		Note 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.

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. • **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

To verify that Support for RFC 3519 NAT Traversal is enabled and functioning properly, perform the following steps.

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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
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

This section contains the following configuration examples:

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
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.

Mobile Networks

Cisco Mobile Networks

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
12.2(4)T3	Support for this feature was introduced for the Cisco 7500 series.
12.2(13)T	Support for dynamic networks was introduced.

This feature module describes the Cisco Mobile Networks feature. It includes the following sections:

Feature Overview

The Cisco Mobile Networks feature enables a mobile router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this mobile router.

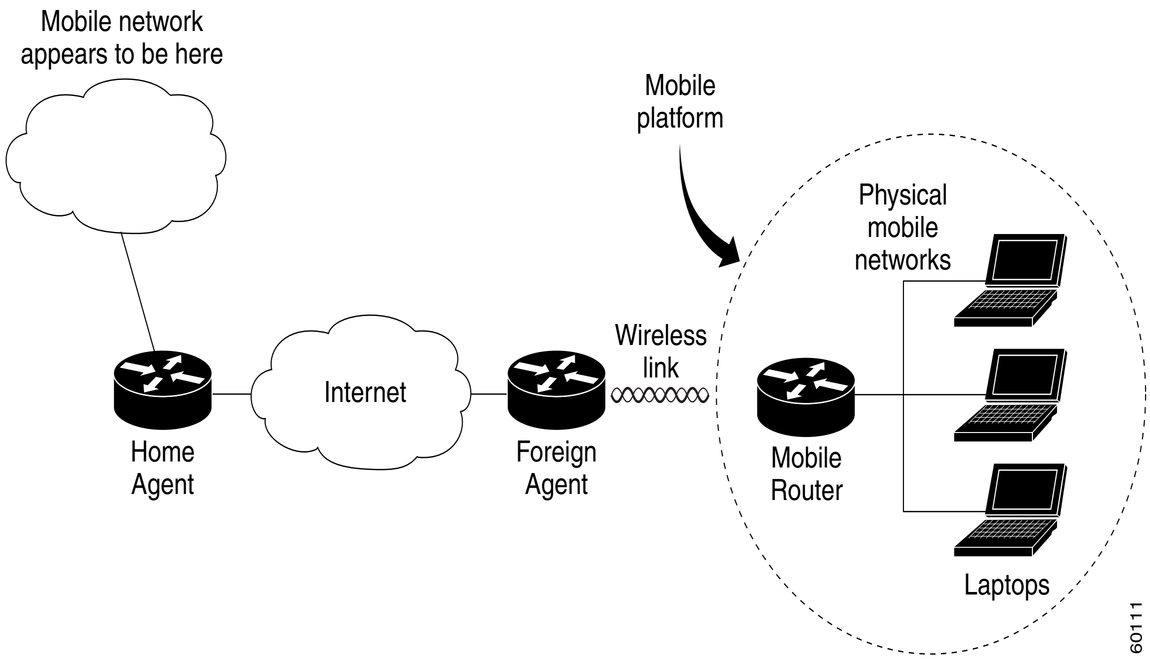
Mobile IP, as defined in standard RFC 3344, provides the architecture that enables the mobile router to connect back to its home network. Mobile IP allows a device to roam while appearing to a user to be at its home network. Such a device is called a mobile node. A mobile node is a node—for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone—that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

maintain ongoing communications while using the same IP address. There is no need for any changes to applications because the solution is at the network layer, which provides the transparent network mobility.

The Cisco Mobile Networks feature comprises three components—the mobile router (MR), home agent (HA), and foreign agent (FA). Figure 1 shows the three components and their relationships within the mobile network.

Figure 1 Cisco Mobile Network Components and Relationships



The mobile router functions similarly to the mobile node with one key difference—the mobile router allows entire networks to roam. For example, an airplane with a mobile router can fly around the world while passengers stay connected to the Internet. This communication is accomplished by Mobile IP aware routers tunneling packets, which are destined to hosts on the mobile networks, to the location where the mobile router is visiting. The mobile router then forwards the packets to the destination device.

These destination devices can be mobile nodes running mobile IP client software or nodes without the software. The mobile router eliminates the need for a mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The mobile router "hides" the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network. See the "Mobile Router" section later in this document for more details on how the mobile router operates.

A home agent is a router on the home network of the mobile router that provides the anchoring point for the mobile networks. The home agent maintains an association between the home IP address of the mobile router and its *care-of address*, which is the current location of the mobile router on a foreign or visited network. The home agent is responsible for keeping track of where the mobile router roams and tunneling packets to the current location of the mobile network. The home agent also injects the mobile networks into its forwarding table. See the "Home Agent" section later in this document for more details on how the home agent operates.

A foreign agent is a router on a foreign network that assists the mobile router in informing its home agent of its current care-of address. It functions as the point of attachment to the mobile router, delivering packets from the home agent to the mobile router. The foreign agent is a fixed router with a direct logical connection to the mobile router. The mobile router and foreign agent need not be connected directly by a physical wireless link. For example, if the mobile router is roaming, the connection between the foreign agent and mobile router occurs on interfaces that are not on the same subnet. This feature does not add any new functionality to the foreign agent component.

Previously, this feature was a static network implementation that supported stub routers only. Cisco IOS Release 12.2(13)T introduces dynamic network support, which means that the mobile router dynamically registers its mobile networks to the home agent, which reduces the amount of configuration required at the home agent. For example, if a home agent supports 2000 mobile routers, the home agent does not need 2000 configurations but only a range of home IP addresses to use for the mobile routers.

This feature implements additional features in the Mobile IP MIB (RFC2006-MIB) to support Cisco Mobile Networks. Prior to this release, mobile node groups in the RFC2006-MIB were not supported.

Cisco IOS Release 12.2(4)T implements mobile node MIB groups from the RFC2006-MIB for the monitoring and management of Cisco Mobile Network activity. Data from managed objects is returned through the use of the **show** commands described in this document, or can be retrieved from a Network Management System using SNMP.

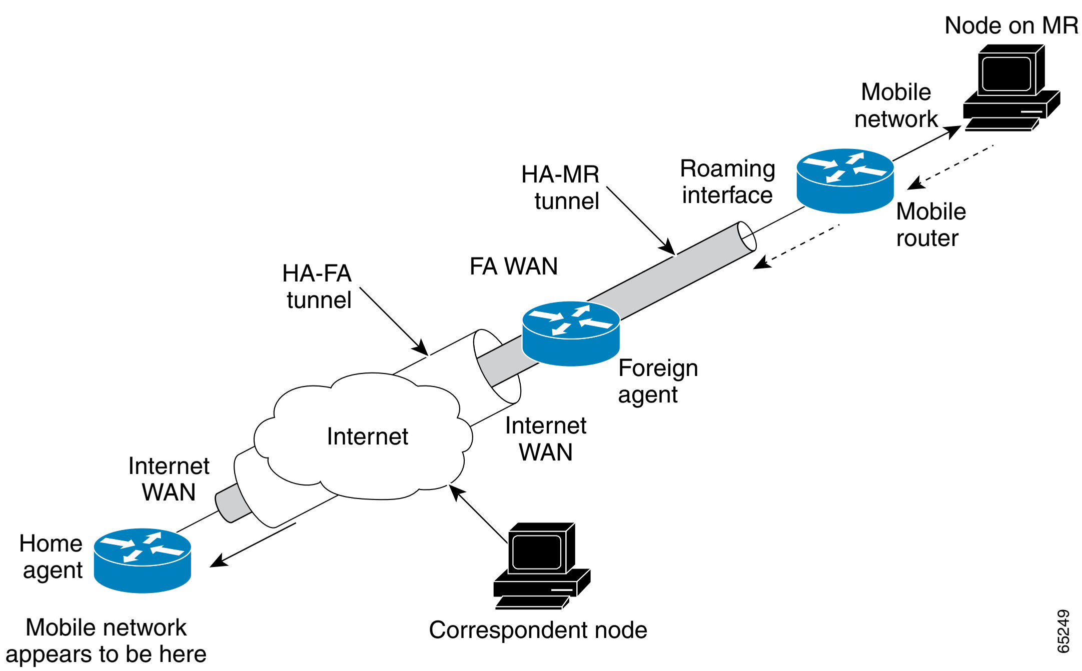
Primary Components of Cisco Mobile Networks

The Cisco Mobile Networks feature introduces the mobile router and adds new functionality to the home agent component as described in the following sections:

- Mobile Router
- Home Agent

Figure 2 shows how packets are routed within the mobile network. The following sections provide more detail on how this routing is accomplished.

Figure 2 Routing Within the Cisco Mobile Network



Mobile Router

Deployed on a mobile platform (such as a car, plane, train, or emergency medical services vehicle), the mobile router functions as a roaming router that provides connectivity for its mobile network. A device connected to the mobile router need not be a mobile node because the mobile router is providing the roaming capabilities.

The mobile router process has three main phases described in the following sections:

- Agent Discovery
- Registration
- Routing

Agent Discovery

During the agent discovery phase, home agents and foreign agents advertise their presence on their attached links by periodically multicasting or broadcasting messages called *agent advertisements*. Agent advertisements are ICMP Router Discovery Protocol (IRDP) messages that convey Mobile IP information. The advertisement contains the IRDP lifetime, which is the number of seconds the agent is considered valid. The advertisement also contains the care-of address, the point of attachment on the foreign network, as well as registration lifetime allowed and supported services such as generic routing encapsulation (GRE), and reverse tunnel.

Agent discovery occurs through periodic advertisements by agents or solicitations by the mobile router.

For periodic advertisements, the mobile router knows that the agent is up as long as it hears the advertisements from the agent. When the mobile router hears the agent advertisements, it keeps track of the agent in an agent table. When the IRDP lifetime expires, the agent is considered disconnected (for example, interface down, out of range, or agent down) and the mobile router removes the agent from its agent table.

Rather than wait for agent advertisements, a mobile router can send an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.

The mobile router receives these advertisements on its interfaces that are configured for roaming and determines if it is connected to its home network or a foreign network. When the mobile router hears an agent advertisement and detects that it has moved outside of its home network, it begins registration, which is the second phase of the process.

Registration

The mobile router is configured with its home address, the IP address or addresses of its home agents, and the mobility security association of its home agent. There is a shared key between the mobile router and the home agent for authentication, as discussed in the "Security for Mobile Networks" section later in this document. The mobile router uses this information along with the information that it learns from the foreign agent advertisements to form a registration request.

The mobile router prefers to register with a particular agent based on the received interface. If more than one interface receives agent advertisements, the one with the highest roaming priority value is preferred. In the case that multiple interfaces have the same priority, the highest bandwidth is preferred. If interfaces have the same bandwidth, the highest interface IP address is preferred.

After determining this preferred path, the mobile router informs the home agent of its current care-of address by sending a registration request. Because the mobile router is attached to a foreign network, the registration request is sent first to the foreign agent.

When the mobile router powers down or determines that it is reconnected to its home link, it deregisters by sending a deregistration request to the home agent.

A successful registration sets up the routing mechanism for transporting packets to and from the mobile networks as the mobile router roams, which is the third phase of the process.

Routing

During the routing or tunneling phase, packets arrive at the home agent. The home agent performs two encapsulations of the packets and tunnels them to the foreign agent. The foreign agent performs one decapsulation and forwards the packets to the mobile router, which performs another decapsulation. The mobile router then forwards the original packets to the IP devices on the mobile networks.

By default, packets from devices on the mobile network arrive at the mobile router, which forwards them to the foreign agent, which routes them normally.

The mobile networks can be statically configured or dynamically registered on the home agent. As the mobile router moves from one foreign agent to another, the mobile router continuously reconfigures the default gateway definition to point to its new path. Although the mobile router can register through different foreign agents, the most recently contacted foreign agent provides the active connection.

A reverse tunnel is when the mobile router tunnels packets to the foreign agent and home agent. In this case, packets from devices arrive at the mobile router, which encapsulates them and then sends them to the foreign agent, which encapsulates the packets and forwards them to the home agent. The home agent decapsulates both encapsulations and routes the original packets.

Home Agent

The home agent provides the anchoring point for the mobile networks. The home agent process has two main phases described in the following sections:

- Registration
- Routing

Registration

After receiving the registration request originated from the mobile router, the home agent checks the validity of the registration request, which includes authentication of the mobile router. If the registration request is valid, the home agent sends a registration reply to the mobile router through the foreign agent.

The home agent also creates a *mobility binding table* that maps the home IP address of the mobile router to the current care-of address of the mobile router. 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 a mobile router (or mobile node) at its home agent.

The home agent processes registration requests from the mobile router in the same way that it does with the mobile node. The only difference is that an additional tunnel is created to the mobile router. Thus, packets destined to the mobile networks are encapsulated twice, as discussed in the "Routing" section that follows. The home agent injects the mobile networks, which are statically defined or dynamically registered, into its forwarding table. This allows routing protocols configured on the home agent to redistribute these mobile routes.

Routing

The home agent advertises reachability to the mobile networks on the mobile router, thereby attracting packets that are destined for them. When a device on the Internet, called a *correspondent node*, sends a packet to the node on the mobile network, the packet is routed to the home agent. The home agent creates tunnels in the following two areas:

- Between the home agent and foreign agent care-of address
- Between the home agent and mobile router

The home agent encapsulates the original packet from the correspondent node twice. The packet arrives at the foreign agent, which decapsulates the HA and FA care-of address tunnel header and forwards the packet to the mobile router, which performs another decapsulation (HA and MR tunnel header) to deliver the packet to the destination node on the mobile network. To the rest of the network, the destination node appears to be located at the home agent; however, it exists physically on the mobile network of the mobile router. See Figure 2 for a graphical representation of how these packets are routed.

Security for Mobile Networks

The home agent of the mobile router is configured with the home IP address of the mobile router and the mobile networks of the mobile router. The message digest algorithm 5 (MD5) hex key is a 128-bit key also defined here. MD5 is an algorithm that takes the registration message and a key to compute the smaller chunk of data called a *message digest*. The mobile router and home agent both have a copy of the key, called a *symmetric key*, and authenticate each other by comparing the results of the computation. If both keys yield the same result, nothing in the packet has changed during transit.

Mobile IP also supports the hash-based message authentication code (HMAC-MD5), which is the default authentication algorithm as of Cisco IOS Release 12.2(13)T.

Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The home agent returns its time stamp to synchronize the mobile router for registration.

Cisco IOS software allows the mobility keys to be stored on an authentication, authorization, and accounting (AAA) server that can be accessed using TACACS+ or RADIUS protocols. Mobile IP in Cisco IOS software also contains registration filters, enabling companies to restrict who is allowed to register.

For more information on security in a Mobile IP environment, refer to the "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

Cisco Mobile Networks Redundancy

The Cisco Mobile Networks feature uses the Hot Standby Router Protocol (HSRP) to provide a full redundancy capability for the mobile router.

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. An HSRP group comprises 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 or more standby home agents that the rest of the topology views as a single virtual home agent.

You must define certain HSRP group attributes on the interfaces of the mobile routers so that Mobile IP can implement the redundancy. The mobile routers are aware of the HSRP states and assume the active or standby role as needed. For more information on mobile router redundancy, see the "Enabling Mobile

Router Redundancy" task later in this document. For more information on home agent redundancy, which is a Cisco proprietary feature that runs on top of HSRP, refer to the "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

HSRP need not be configured on the foreign agent. Foreign agent redundancy is achieved by overlapping wireless coverage.

Benefits

Mobility Solution at the Network Layer

With the mobile router deployed in a moving vehicle, repeated reconfiguration of the various devices attached to that router as the vehicle travels is no longer necessary. Because the mobile router operates at the network layer and is independent of the physical layer, it operates transparently over cellular, satellite, and other wireless or fixed media.

Always-On Connection to the Internet

This feature supports an always-on connection to the Internet, providing access to current and changing information. For example, aircraft pilots can access the latest weather updates while flying and EMS vehicles can be in communication with emergency room technicians while on the way to the hospital.

Versatile

Any IP-enabled device can be connected to the mobile router LAN ports and achieve mobility. Applications that are not specifically designed for mobility can be accessed and deployed.

Dynamic Mobile Networks

The dynamic network enables dynamic registration of mobile networks, which results in minimal configuration on the home agent making administration and set up easier. When configured for dynamic registration, the mobile router tells the home agent which networks are configured in each registration request. The home agent dynamically adds these networks to the forwarding table and there is no need to statically define the networks on the home agent.

Preferred Path

By using the preferred path, a network designer can specify the primary link, based upon bandwidth or priority, to reduce costs or to use a specific carrier.

Standards-Based Solution

Mobile IP complies with official protocol standards of the Internet.

Mobile IP MIB Support

Support for mobile node MIB groups in the Mobile IP MIB allows the monitoring of Mobile Network activity using the Cisco IOS command line interface or SNMP. For further details, refer to the RFC2006-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/, and RFC 2006, *The Definitions of Managed Objects for IP Mobility Support using SMIv2*.

Related Features and Technologies

Mobile IP is documented in the *Cisco IOS IP Configuration Guide*. Mobile IP configuration commands are documented in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

Related Documents

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.2
- *Cisco IOS IP Configuration Guide,* Release 12.2
- *Cisco Mobile Networks—Asymmetric Link Support*, Release 12.2(13)T

Supported Platforms

- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620 router
- Cisco 3640 router
- Cisco 3660 router
- Cisco 7200 series
- Cisco 7500 series (Cisco IOS Release 12.2(4)T2 and later releases)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, 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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

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

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

- 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*
- RFC 3344, *IP Mobility Support for IPv4*

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.

Configuration Tasks

See the following sections for configuration tasks for the Cisco Mobile Networks feature. Each task in the list is identified as either required or optional.

- Enabling Home Agent Services (required)

- Enabling Foreign Agent Services (required)
- Enabling Mobile Router Services (required)
- Enabling Mobile Router Redundancy (optional)
- Verifying Home Agent Configuration (optional)
- Verifying Foreign Agent Configuration (optional)
- Verifying Mobile Router Configuration (optional)
- Verifying Mobile Router Redundancy (optional)

Enabling Home Agent Services

You can configure a home agent with both dynamically registered and statically configured mobile networks. However, a statically configured mobile network will always take precedence over dynamic registrations of the same network.

To enable home agent services on the router, use the following commands beginning in global configuration mode:

	Command	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`** `[`**`address`** *`ip-address`*`][`**`broadcast`**`] [`**`care-of-access`** *`acl`*`] [`**`lifetime`** *`number`*`] [`**`replay`** *`seconds`*`] [`**`reverse-tunnel-off`**`] [`**`roam-access`** *`acl`*`] [`**`suppress-unreachable`**`]`	Enables home agent service.
Step 4	`Router(config)#` **`ip mobile virtual-network`** *`net mask`* `[`**`address`** *`address`*`]`	Defines a virtual network. Specifies that the home network is a virtual network, which means that the mobile router is not physically attached to the home agent. Adds the network to the home agent's forwarding table so that routing protocols can redistribute the subnet. If not using virtual networks, go to step 8.
Step 5	`Router(config-router)#` **`router`** *`protocol`*	Configures a routing protocol.
Step 6	`Router(config)#` **`redistribute mobile`** `[`**`metric`** *`metric-value`*`] [`**`metric-type`** *`type-value`*`]`	Enables redistribution of a virtual network into routing protocols.
Step 7	`Router(config-router)#` **`exit`**	Returns to global configuration mode.
Step 8	`Router(config)#` **`ip mobile host`** *`lower`* `[`*`upper`*`] {`**`interface`** *`name`* `|` **`virtual-network`** *`net mask`*`} [`**`lifetime`** *`number`*`]`	Configures the mobile router as a mobile host. The IP address is in the home network. The **interface** *name* option configures a physical connection from the home agent to the mobile router.

	Command	Purpose
Step 9	Router(config)# **ip mobile mobile-networks** *lower* [*upper*]	Configures mobile networks for the mobile host and enters mobile networks configuration mode. The *upper* range can be used only with dynamically registered networks and allows you to configure multiple mobile routers at once. The range must match the range configured in the **ip mobile host** command.
Step 10	Router(mobile-networks)# **description** *string*	(Optional) Adds a description to a mobile router configuration.
Step 11	Router(mobile-networks)# **network** *net mask*	(Optional) Configures a network that is attached to the mobile router as a mobile network. Use this command to statically configure networks.
Step 12	Router(mobile-networks)# **register**	(Optional) Dynamically registers the mobile networks with the home agent. The home agent learns about the mobile networks through this registration process. When the mobile router registers its mobile networks on the home agent, the home agent looks up the mobile network configuration and verifies that the **register** command is configured before adding forwarding entries to the mobile networks. If the **register** command is not configured, the home agent will reject an attempt by the mobile router to dynamically register its mobile networks.
Step 13	Router(mobile-networks)# **exit**	Exits mobile networks configuration mode.
Step 14	Router(config)# **ip mobile secure host** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*	Sets up mobile host security associations. This is the security association the mobile router uses when sending in a registration request. The SPI and key between the home agent and mobile router are known. The address is the home IP address of the mobile router.

Enabling Foreign Agent Services

There are no changes to the foreign agent configuration with the introduction of dynamic network support.

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

	Command	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.

	Command	Purpose
Step 3	`Router(config)#` **`ip mobile foreign-agent care-of`** *`interface`*	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 4	`Router(config)#` **`interface`** *`type number`*	Configures an interface and enters interface configuration mode.
Step 5	`Router(config-if)#` **`ip address`** *`ip-address mask`*	Sets a primary IP address of the interface.
Step 6	`Router(config-if)#` **`ip irdp`**	Enables IRDP processing on an interface.
Step 7	`Router(config-if)#` **`ip irdp maxadvertinterval`** *`seconds`*	(Optional) Specifies maximum interval in seconds between advertisements.
Step 8	`Router(config-if)#` **`ip irdp minadvertinterval`** *`seconds`*	(Optional) Specifies minimum interval in seconds between advertisements.
Step 9	`Router(config-if)#` **`ip irdp holdtime`** *`seconds`*	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the **maxadvertinterval** period.
Step 10	`Router(config-if)#` **`ip mobile foreign-service`**	Enables foreign agent service on an interface. This will also append Mobile IP information such as care-of address, lifetime, and service flags to the advertisement.

Enabling Mobile Router Services

To enable mobile router services, use the following commands beginning in global configuration mode:

	Command	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 router`**	Enables the mobile router and enters mobile router configuration mode.
Step 4	`Router(mobile-router)#` **`address`** *`address mask`*	Sets the home IP address and network mask of the mobile router.
Step 5	`Router(mobile-router)#` **`home-agent`** *`ip-address`*	Specifies the home agent that the mobile router uses during registration.
Step 6	`Router(mobile-router)#` **`mobile-network`** *`interface`*	(Optional) Specifies the mobile router interface that is connected to the dynamic mobile network. There can be more than one mobile network configured on a mobile router. The mobile router's registrations will contain these mobile networks.

	Command	Purpose
Step 7	Router(mobile-router)# **register** {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}	(Optional) Controls the registration parameters of the mobile router.
Step 8	Router(mobile-router)# **reverse-tunnel**	(Optional) Enables the reverse tunnel function.
Step 9	Router(mobile-router)# **exit**	Exits mobile router configuration mode.
Step 10	Router(config)# **ip mobile secure home-agent** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*	Sets up home agent security associations. The SPI and key between the mobile router and home agent are known. The address is the home IP address of the home agent.
Step 11	Router(config)# **interface** *type number*	Configures an interface and enters interface configuration mode.
Step 12	Router(config-if)# **ip address** *ip-address mask*	Sets a primary IP address of the interface.
Step 13	Router(config-if)# **ip mobile router-service** {**hold-down** *seconds* | **roam** [**priority** *value*] | **solicit** [**interval** *seconds*] [**retransmit initial** *min* **maximum** *seconds* **retry** *number*]}	Enables mobile router service, such as roaming, on an interface.

Enabling Mobile Router Redundancy

To enable mobile router redundancy, use the following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	Enables the HSRP.
Step 2	Router(config-if)# **standby priority** *priority*	Sets the Hot Standby priority used in choosing the active router.
Step 3	Router(config-if)# **standby preempt**	Configures the router to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router.
Step 4	Router(config-if)# **standby name** *group-name*	Configures the name of the standby group.
Step 5	Router(config-if)# **standby** [*group-number*] **track** *interface-type interface-number* [*interface-priority*]	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces. The *interface-priority* argument specifies the amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.
Step 6	Router(config-if)# **exit**	Exits interface configuration mode.

	Command	Purpose
Step 7	`Router(config)#` **`ip mobile router`**	Enables the mobile router.
Step 8	`Router(mobile-router)#` **`redundancy group`** *`name`*	Configures fault tolerance for the mobile router. The *name* argument must match the name specified in the **standby name** *group-name* command.

You need not configure HSRP on both the mobile router's roaming interface and the interface attached to the physical mobile networks. If one of the interfaces is configured with HSRP, and the **standby track** command is configured on the other interface, the redundancy mechanism will work. See the "Cisco Mobile Network Redundancy Example" section for a configuration example.

Verifying Home Agent Configuration

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

Command	Purpose
`Router#` **`show ip mobile mobile-networks`** `[`*`address`*`]`	Displays a list of mobile networks associated with the mobile router.
`Router#` **`show ip mobile host`** `[`*`address`*`]`	Displays mobile node information.
`Router#` **`show ip mobile secure host`** `[`*`address`*`]`	Displays the mobility security associations for the mobile host.

Verifying Foreign Agent Configuration

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

Command	Purpose
`Router#` **`show ip mobile global`**	Displays global information for mobile agents.
`Router#` **`show ip mobile interface`**	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

Verifying Mobile Router Configuration

To verify the mobile router configuration, use the following commands in privileged EXEC mode as needed:

Command	Purpose
`Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
`Router# show ip mobile router traffic`	Displays the counters that the mobile router maintains.

Verifying Mobile Router Redundancy

To verify that mobile router redundancy is configured correctly on the router, use the following commands in privileged EXEC mode, as needed:

Command	Purpose
`Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
`Router# show ip mobile router traffic`	Displays the counters that the mobile router maintains.
`Router# show standby`	Displays HSRP information.

Troubleshooting Tips

- Adjust the agent advertisement interval value on the foreign agent using the **ip irdp maxadvertinterval** *seconds* interface configuration command. Begin by setting the timer to 10 seconds and adjust as needed.
- Before you can ping a subnet on the mobile router, the mobile router must be registered with the home agent and the mobile network (subnet) must be statically configured or dynamically registered on the home agent.
- Use extended pings for roaming interfaces. The pings from the mobile router need to have the home address of the mobile router as the source address in the extended ping. Standard pings will have the source address of the roaming interface as the source address, which is not routeable from the standpoint of the rest of the network unless the roaming interfaces are statically configured on the home agent.
- Redistribute mobile subnets on the home agent so that return traffic can be sent back to the mobile router. Most routing protocols require that default metrics be configured for redistribution.
- Establish a return route from the foreign agent to the home agent.
- Avoid placing any routers behind the mobile router because the mobile router functions as a stub router.
- A statically configured mobile network takes precedence over the same dynamically registered mobile network.
- A mobile network can be configured or registered by only one mobile router at a time.

Monitoring and Maintaining the Mobile Router

To monitor and maintain the mobile router, use the following commands in privileged EXEC mode, as needed:

Command	Purpose
`Router# clear ip mobile router agent`	Deletes learned agents and the corresponding care-of address of the foreign agent from the mobile router agent table.
`Router# clear ip mobile router registration`	Deletes registration entries from the mobile router registration table.
`Router# clear ip mobile router traffic`	Clears the counters that the mobile router maintains.
`Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
`Router# show ip mobile router agent`	Displays information about the agents for the mobile router.
`Router# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming.
`Router# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
`Router# show ip mobile router traffic`	Displays counters that the mobile router maintains.
`Router# debug ip mobile router [detail]`	Displays debug messages for the mobile router.

Configuration Examples

This section provides the following configuration examples:

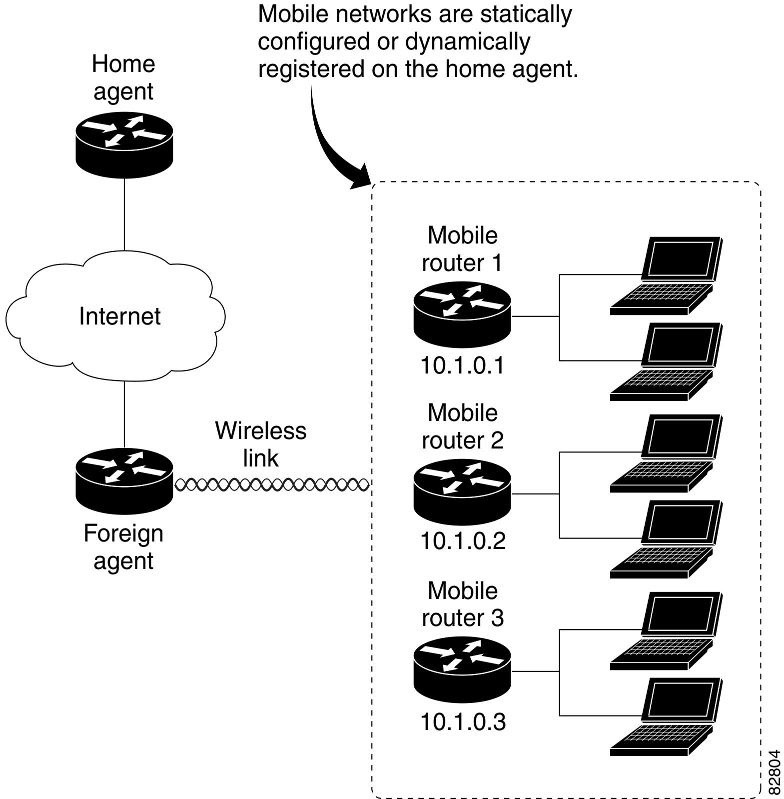
- Home Agent Example
- Foreign Agent Example
- Mobile Router Example
- Cisco Mobile Network Redundancy Example

In the following examples, a home agent provides service for three mobile routers. Each mobile router has a satellite link and wireless LAN link when roaming. Each is allocated a network that can be partitioned further.

The mobile networks on the mobile routers are both statically configured and dynamically registered on the home agent while the mobile routers roam via foreign agents.

See Figure 3 for an example topology.

Figure 3 Topology Showing Home Agent Supporting Three Mobile Routers



Home Agent Example

In the following example, a home agent provides service for three mobile routers. Note that the home agent will advertise reachability to the virtual networks.

```
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
router mobile
!
! Virtual network advertised by HA is the home network of the MR
ip mobile virtual-network 10.1.0.0 255.255.0.0
ip mobile host 10.1.0.1 virtual-network 10.1.0.0 255.255.0.0
ip mobile host 10.1.0.2 virtual-network 10.1.0.0 255.255.0.0
ip mobile host 10.1.0.3 10.1.0.10 virtual-network 10.1.0.0 255.255.0.0 aaa load-sa
!
! Associated host address that informs HA that 10.1.0.1 is actually an MR
ip mobile mobile-networks 10.1.0.1
! Static config of MR's mobile networks
 description jet
 network 172.6.1.0 255.255.255.0
 network 172.6.2.0 255.255.255.0
!
! Associated host address that informs HA that 10.1.0.2 is actually an MR
ip mobile mobile-networks 10.1.0.2
! One static mobile network; MR may also dynamically register mobile nets
 description ship
 network 172.7.1.0 255.255.255.0
```

```
 register
!
! Range of hosts that are MRs
ip mobile mobile-networks 10.1.0.3 10.1.0.10
! All can dynamically register their mobile networks
 register
!
ip mobile secure host 10.1.0.1 spi 101 key hex 12345678123456781234567812345678
ip mobile secure host 10.1.0.2 spi 102 key hex 23456781234567812345678123456781
```

Foreign Agent Example

In the following example, the foreign agent is providing service on serial interface 0:

```
router mobile
ip mobile foreign-agent care-of serial0
!
interface serial0
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 12
 ip mobile foreign-service
```

Mobile Router Example

In the following example, three mobile routers provide services for the mobile networks:

Mobile Router 1

```
interface loopback0
! MR home address
 ip address 10.1.0.1 255.255.255.255
!
interface serial 0
! MR roaming interface
 ip address 172.21.58.253 255.255.255.252
 ip mobile router-service roam
interface ethernet 0
! MR roaming interface
 ip address 172.21.58.249 255.255.255.252
 ip mobile router-service roam
interface ethernet 1
 ip address 172.6.1.1 255.255.255.0
interface ethernet 2
 ip address 172.6.2.1 255.255.255.0
!
!
router mobile
ip mobile router
 address 10.1.0.1 255.255.0.0
 home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 101 key hex 12345678123456781234567812345678
```

Mobile Router 2

```
interface loopback0
! MR home address
 ip address 10.1.0.2 255.255.255.255
!
interface serial 0
! MR roaming interface
 ip address 172.21.58.245 255.255.255.252
 ip mobile router-service roam
interface ethernet 0
! MR roaming interface
 ip address 172.21.58.241 255.255.255.252
 ip mobile router-service roam
interface ethernet 1
 ip address 172.7.1.1 255.255.255.0
interface ethernet 2
 ip address 172.7.2.1 255.255.255.0
!
!
router mobile
ip mobile router
 address 10.1.0.2 255.255.0.0
 home-agent 1.1.1.1
 mobile-network ethernet 2
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781
```

Mobile Router 3

```
interface loopback0
! MR home address
 ip address 10.1.0.3 255.255.255.255
!
interface serial 0
! MR roaming interface
 ip address 172.21.58.237 255.255.255.252
 ip mobile router-service roam
interface ethernet 0
! MR roaming interface
 ip address 172.21.58.233 255.255.255.252
 ip mobile router-service roam
interface ethernet 1
 ip address 172.8.1.1 255.255.255.0
interface ethernet 2
 ip address 172.8.2.1 255.255.255.0
!
!
router mobile
ip mobile router
 address 10.1.0.3 255.255.0.0
 home-agent 1.1.1.1
 mobile-network ethernet 1
 mobile-network ethernet 2
ip mobile secure home-agent 1.1.1.1 spi 103 key hex 45678234567812312345678123456781
!
```

Cisco Mobile Network Redundancy Example

There can be three levels of redundancy for the Cisco Mobile Network: home agent redundancy, foreign agent redundancy, and mobile router redundancy.

In the home agent example, two home agents provide redundancy for the home agent component. If one home agent fails, the standby home agent immediately becomes active so that no packets are lost. HSRP is configured on the home agents, along with HSRP attributes such as the HSRP group name. Thus, the rest of the topology treats the home agents as a single virtual home agent and any fail-over is transparent.

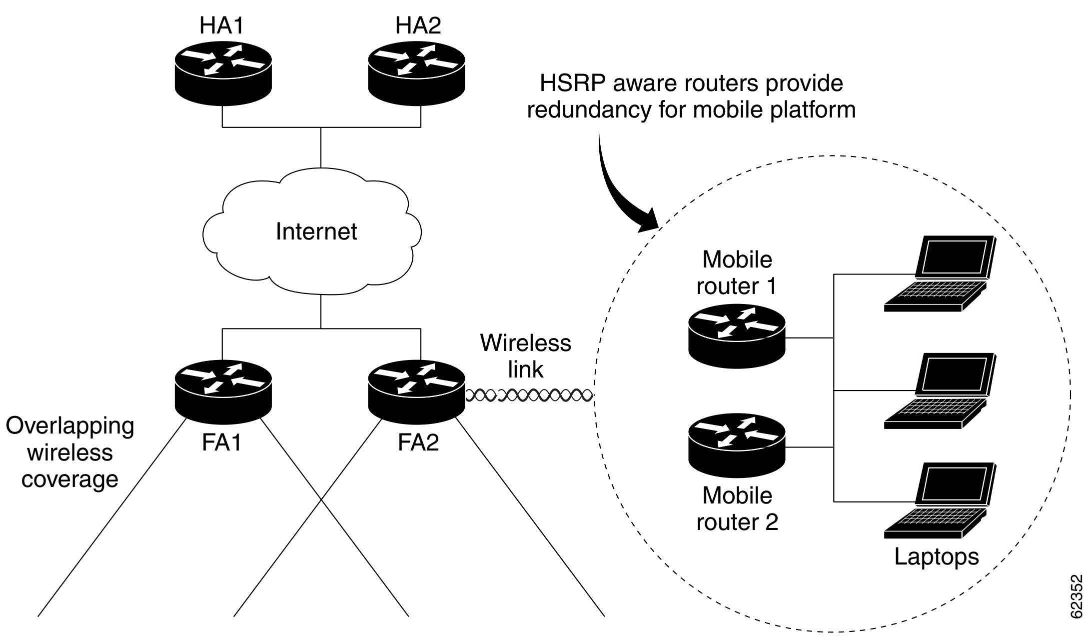
The mobile networks also are defined on the home agent so that the home agent knows to inject these networks into the routing table when the mobile router is registered.

In the foreign agent example, two routers provide foreign agent services. No specific redundancy feature needs to be configured on foreign agents; overlapping wireless coverage provides the redundancy.

The mobile routers use HSRP to provide redundancy, and their group name is associated to the HSRP group name. The mobile routers are aware of the HSRP states. When HSRP is in the active state, the mobile router is active. If HSRP is in the nonactive state, the mobile router is passive. When an active mobile router fails, the standby mobile router becomes active and sends out solicitations out its roaming interfaces to learn about foreign agents and register.

See Figure 4 for an example topology of a redundant network where two mobile routers are connected to each other on a LAN with HSRP enabled.

Figure 4 Topology Showing Cisco Mobile Networks Redundancy



Home Agent 1 (HA1) Configuration

```
interface Ethernet1/1
 ip address 100.100.100.3 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 duplex half
 standby ip 100.100.100.1
 standby priority 100
 standby preempt delay sync 60
!HSRP group name
 standby name HA_HSRP2
!
```

```
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent
! Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network address 100.100.100.1
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
ip mobile mobile-networks 70.70.70.70
 description san jose jet
! Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.2 spi 300 key hex 12345678123496781234567812345678
```

Home Agent 2 (HA2) Configuration

```
interface Ethernet1/1
 ip address 100.100.100.2 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 standby ip 100.100.100.1
 standby priority 95
 standby preempt delay sync 60
! HSRP group name
 standby name HA_HSRP2
!
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent
!Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network address 100.100.100.1
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
ip mobile mobile-networks 70.70.70.70
 description san jose jet
!Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.1 spi 300 key hex 12345978123456781234567812345678
```

Foreign Agent 1 (FA1) Configuration

```
interface Ethernet0
 ip address 171.69.68.2 255.255.255.0
 media-type 10BaseT
!
```

```
interface Ethernet1
 ip address 80.80.80.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 ip mobile foreign-service
 media-type 10BaseT
!
router mobile
!
router rip
 version 2
 network 80.0.0.0
 network 100.0.0.0
!
ip classless
no ip http server
ip mobile foreign-agent care-of Ethernet1
```

Foreign Agent 2 (FA2) Configuration

```
interface Ethernet1
 ip address 171.69.68.1 255.255.255.0
 media-type 10BaseT
!
interface Ethernet2
 ip address 80.80.80.2 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 ip mobile foreign-service
 media-type 10BaseT
!
router mobile
!
router rip
 version 2
 network 80.0.0.0
 network 100.0.0.0
!
ip classless
no ip http server
ip mobile foreign-agent care-of Ethernet2
```

Mobile Router 1 Configuration

```
interface Ethernet5/2
! MR roaming interface
 ip address 70.70.70.4 255.255.255.0
 ip mobile router-service roam
! Configure redundancy for mobile router using HSRP
 standby ip 70.70.70.70
 standby priority 105
 standby preempt
 standby name MR_HSRP2
 standby track Ethernet5/4
!
interface Ethernet5/4
! Interface to Mobile Network
 ip address 20.20.20.2 255.255.255.0
!
router mobile
```

```
!
router rip
 version 2
 passive-interface Ethernet5/2
 network 20.0.0.0
 network 70.0.0.0
!
ip classless
no ip http server
ip mobile secure home-agent 100.100.100.100 spi 100 key hex
12345678123456781234567812345678
ip mobile router
! Maps to HSRP group name
 redundancy group MR_HSRP2
! Using roaming interface hot address as MR address
 address 70.70.70.70 255.255.255.0
 home-agent 100.100.100.1
```

Mobile Router 2 Configuration

```
interface Ethernet1/2
! MR roaming interface
 ip address 70.70.70.3 255.255.255.0
 ip mobile router-service roam
! Configure redundancy for mobile router using HSRP
 standby ip 70.70.70.70
 standby priority 100
 standby preempt
 standby name MR_HSRP2
 standby track Ethernet1/4
!
interface Ethernet1/4
! Interface to Mobile Network
ip address 20.20.20.1 255.255.255.0
!
router mobile
!
router rip
 version 2
 passive-interface Ethernet1/2
 network 20.0.0.0
 network 70.0.0.0
!
ip classless
no ip http server
ip mobile secure home-agent 100.100.100.100 spi 100 key hex
12345678123456781234567812345678
ip mobile router
! Maps to HSRP group name
 redundancy group MR_HSRP2
! Using roaming interface hot address as MR address
 address 70.70.70.70 255.255.255.0
 home-agent 100.100.100.1
```

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*.

- **address (mobile router)**
- **clear ip mobile router agent**
- **clear ip mobile router registration**
- **clear ip mobile router traffic**
- **debug ip mobile**
- **debug ip mobile router**
- **description (mobile networks)**
- **home-agent**
- **ip mobile mobile-networks**
- **ip mobile router**
- **ip mobile router-service**
- **mobile-network**
- **network (mobile networks)**
- **redundancy group**
- **register (mobile networks)**
- **register (mobile router)**
- **reverse-tunnel**
- **show ip mobile binding**
- **show ip mobile host**
- **show ip mobile mobile-networks**
- **show ip mobile router**
- **show ip mobile router agent**
- **show ip mobile router interface**
- **show ip mobile router registration**
- **show ip mobile router traffic**

Glossary

agent advertisement—An advertisement message constructed by an attachment of a special extension to a ICMP Router Discovery Protocol (IRDP).

agent discovery—The method by which a mobile node or mobile router determines whether it is currently connected to its home network or a foreign network and detects whether it has moved and the way it has moved. It is the mechanism by which mobile nodes or mobile routers query and discover mobility agents. Agent discovery is an extension to ICMP Router Discovery Protocol (IRDP) (RFC 1256), which includes a mechanism to advertise mobility services to potential users.

agent solicitation—A request for an agent advertisement sent by the mobile node or mobile router.

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.

correspondent node—A peer with which a mobile node is communicating. A correspondent node may be either stationary or mobile.

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.

foreign network—Any network other than the home network of the mobile node.

home address—An IP address that is assigned for an extended time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

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*.

home network—The network, possibly virtual, whose network prefix equals the network prefix of the home address of a mobile node.

link—A facility or medium over which nodes communicate at the link layer. A link underlies the network layer.

link-layer address—The address used to identify an endpoint of some communication over a physical link. Typically, the link-layer address is a MAC address of an interface.

mobility agent—A home agent or a foreign agent.

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

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

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.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

mobility security association—A collection of security contexts between a pair of nodes that may be applied to Mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode, a secret (a shared key or appropriate public/private key pair), and a style of replay protection in use.

MTU—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

node—A host or router.

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. Registration may happen directly from the mobile node to the home agent or through a foreign agent.

roaming interface—An interface used by the mobile router to detect foreign agents and home agents while roaming. Registration and traffic occur on the interface.

SPI—security parameter index. The index identifying a security context between a pair of nodes. On the home agent, the SPI identifies which shared secret to use to compute the md5 hash value.

tunnel—The path followed by a packet while it is encapsulated from the home agent to the mobile node. The model is that, while it is encapsulated, a packet is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

virtual network—A network with no physical instantiation beyond a router (with a physical network interface on another network). The router (a home agent, for example) generally advertises reachability to the virtual network using conventional routing protocols.

visited network—A network other than the home network of a mobile node, to which the mobile node is currently connected.

visitor list—The list of mobile nodes visiting a foreign agent.

Cisco Mobile Networks—Asymmetric Link

An asymmetric link environment such as satellite communications, with a separate uplink and downlink, provides challenges for the mobile router and foreign agent. Because each unidirectional link provides only one way traffic, the inherent mapping in the foreign agent of the return path to the mobile router for incoming messages does not apply. The Cisco Mobile Networks—Asymmetric Link feature solves this problem by extending the use of mobile networks to networks where the mobile router has unidirectional links to the foreign agent. The foreign agent is able to transmit packets back to the mobile router over a different link than the one on which it receives packets from the mobile router.

Feature Specifications for the Cisco Mobile Networks—Asymmetric Link

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

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases have in common.

To access Cisco Feature Navigator, 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 at the following URL:

http://www.cisco.com/register

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Contents

Restrictions for Cisco Mobile Networks—Asymmetric Link

This feature can be used only on serial interfaces.

Information About Cisco Mobile Networks—Asymmetric Link

To configure the Cisco Mobile Networks—Asymmetric Link feature, you need to understand the following concept:

- Unidirectional Routing in Cisco Mobile Networks, page 2

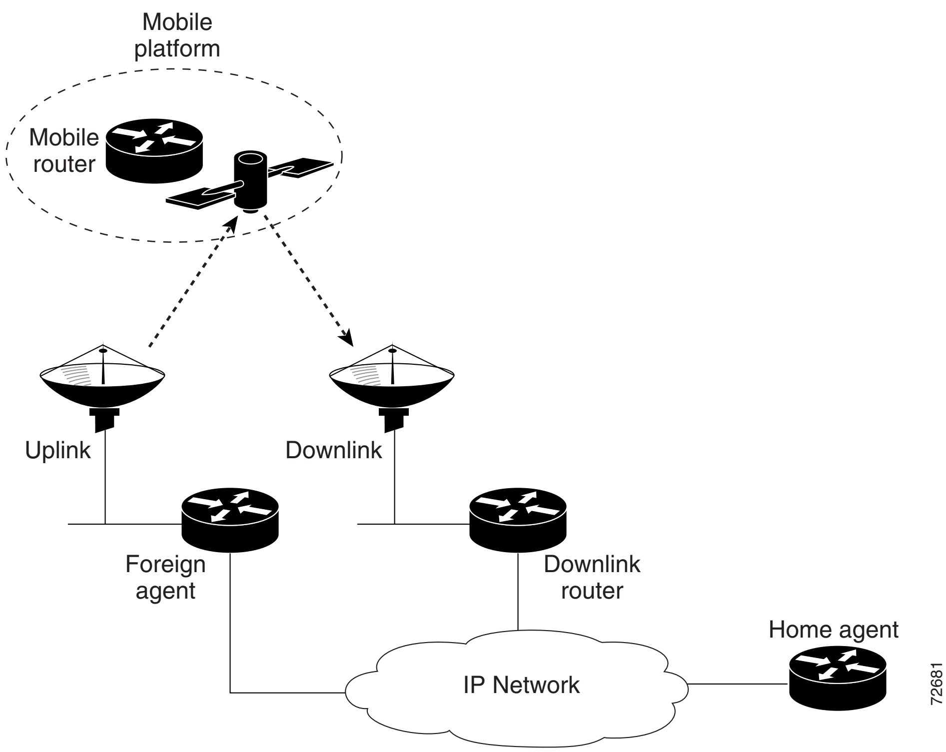
Unidirectional Routing in Cisco Mobile Networks

With unidirectional routing, registration requests from the mobile router travel a slightly different route than in bidirectional routing. The mobile router uses different interfaces to transmit and receive. Advertisements are received on the mobile router interface that is connected to the uplink equipment. This interface is configured to be receive-only (**transmit-interface** command) and another interface connected to the downlink traffic is configured to be transmit-only. When the mobile router receives an advertisement from the foreign agent on the uplink, it takes the care-of address advertised by that foreign agent to use in the registration request. However, the mobile router has been configured to send traffic to a downlink router even though it hears advertisements on the interface connected to the uplink equipment. The registration request is sent out the mobile router's downlink interface to the care-of address given in the the foreign agent's uplink interface.

The downlink router routes the registration request using normal routing to the foreign agent. When the foreign agent receives the registration request, it looks up the care-of address. If the care-of address is associated with an asymmetric interface, the foreign agent treats the mobile router as a visitor on that interface and forwards the registration request to the home agent. The home agent sends a registration reply to the foreign agent care-of address, which will then be forwarded to the mobile router through the uplink interface.

Figure 1 shows how packets are routed within the mobile network using unidirectional routing.

Figure 1 Unidirectional Routing in an Asymmetric Communications Environment



How to Configure Mobile Networks in an Asymmetric Link Environment

This section contains the following procedures:

- Enabling Mobile Router Services for Unidirectional Interfaces, page 4 (required)
- Enabling Foreign Agent Services for Unidirectional Interfaces, page 5 (required)
- Enabling Home Agent Services, page 7 (required)
- Verifying Cisco Mobile Networks—Asymmetric Link Configuration, page 7 (optional)

Enabling Mobile Router Services for Unidirectional Interfaces

To configure this task of enabling mobile router services for a unidirectional interface, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface** *type number*
4. **transmit-interface** *type number*
5. **ip address** *ip-address mask*
6. **ip mobile router-service roam**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip mobile router-service roam**

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	**interface** *type number* **Example:** `Router(config)# interface serial 1`	Configures an interface type and enters interface configuration mode.
Step 4	**transmit-interface** *type number* **Example:** `Router(config-if)# transmit-interface serial 2`	Assigns a transmit interface to a receive-only interface. • This is the uplink (receive-only) interface. • In the example, this command specifies interface serial 2, connected to the downlink router, to be the transmit-only interface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.6.2 255.255.255.0`	Sets a primary IP address for an interface. • This is the IP address of a roaming interface.

	Command or Action	Purpose
Step 6	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables the mobile router to specify on which configured interface it will discover foreign agents.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface serial 2`	Configures an interface type and enters interface configuration mode. • This is the downlink (transmit-only) interface that was specified in Step 4.
Step 9	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.7.2 255.255.255.0`	Sets a primary IP address for an interface. • This is the IP address of a roaming interface.
Step 10	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables the mobile router to specify on which configured interface it will discover foreign agents.

Troubleshooting Tips

- With back-to-back serial interfaces (DTE to DTE), you need to disable keepalives with the **no keepalive** interface configuration command.
- The forwarding table will appear “normal.” Use the **debug ip packet** and **trace** commands to display the packets that are being routed unidirectionally.

Enabling Foreign Agent Services for Unidirectional Interfaces

To enable foreign agent services for unidirectional interfaces, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip irdp**
6. **ip irdp maxadvertinterval** *seconds*
7. **ip irdp minadvertinterval** *seconds*

8. **ip irdp holdtime** *seconds*
9. **ip mobile foreign-service**
10. **exit**
11. **router mobile**
12. **exit**
13. **ip mobile foreign-agent** [**care-of** *interface* [**interface-only transmit-only**]]

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	**interface** *type number* **Example:** `Router(config)# interface serial 1`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.2 255.255.255.0`	Sets a primary IP address of the interface.
Step 5	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables IRDP processing on an interface.
Step 6	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 4`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 7	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 3`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 8	**ip irdp holdtime** *seconds* **Example:** `Router(config-if)# ip irdp holdtime 10`	(Optional) Length of time in seconds that advertisements are held valid. • Default is three times the **maxadvertinterval** period.

	Command or Action	Purpose
Step 9	**ip mobile foreign-service** **Example:** `Router(config-if)# ip mobile foreign-service`	Enables foreign agent service on an interface. • This command also appends Mobile IP information such as care-of address, lifetime, and service flags to the advertisement.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 11	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 12	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 13	**ip mobile foreign-agent** [**care-of** *interface* [**interface-only transmit-only**]] **Example:** `Router(config)# ip mobile foreign-agent care-of serial 1 interface-only transmit-only`	Enables foreign agent service. • The **interface-only** keyword causes the interface type specified in the *interface* argument to advertise only its own address as the care-of address. • The **transmit-only** keyword informs Mobile IP that the interface acts as an uplink so for registration and reply purposes, treat registration requests received for this care-of address as having arrived on the transmit-only interface. • Any care-of address can be configured as interface only but only serial interfaces can be configured as transmit only.

Enabling Home Agent Services

There are no changes to the home agent configuration with the introduction of the Cisco Mobile Neworks—Asymmetric Link feature. Configure the home agent as described in the "Cisco Mobile Networks" feature document introduced in Cisco IOS Release 12.2(4)T.

Verifying Cisco Mobile Networks—Asymmetric Link Configuration

To verify that the asymmetric link configuration on the foreign agent is working, perform the following optional steps:

SUMMARY STEPS

1. **show ip mobile visitor**
2. **show ip mobile globals**

3. **show ip mobile interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`show ip mobile visitor`** **Example:** `Router# show ip mobile visitor`	Displays the table containing the visitor list of the foreign agent.
Step 2	**`show ip mobile globals`** **Example:** `Router# show ip mobile globals`	Displays global information for mobile agents. • Relevant fields in the display output will indicate interface-only and transmit-only status if configured. • See the display output following this table for an example.
Step 3	**`show ip mobile interface`** **Example:** `Router# show ip mobile interface`	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

The following example shows interface-only and transmit-only configured on the foreign agent:

```
Router# show ip mobile globals

IP Mobility global information:

Home Agent is not enabled

Foreign Agent

   Pending registrations expire after 15 secs
   Care-of addresses advertised
    Serial4/0 (11.0.0.2) - up, interface-only, transmit-only
```

Configuration Examples for Cisco Mobile Networks—Asymmetric Link

This section provides the following configuration examples:

- Mobile Router Example, page 8
- Foreign Agent Example, page 9

In the following examples, a home agent provides service for one mobile router. The mobile router detects the foreign agent advertisements on the uplink interface and sends the registration request on the downlink interface to the advertised care-of address of the foreign agent.

Mobile Router Example

The following example shows the mobile router configuration:

```
!
interface Loopback1
 ip address 20.0.4.1 255.255.255.0
!
interface Serial3/0
! Uplink interface
 transmit-interface Serial3/1
  ip address 11.0.0.1 255.255.255.0
 ip mobile router-service roam
!
interface Serial3/1
! Downlink interface
 ip address 12.0.0.1 255.255.255.
 ip mobile router-service roam
!
router mobile
!
ip mobile secure home-agent 43.0.0.3 spi 100 key hex 11223344556677881122334455667788
ip mobile router
address 20.0.4.1 255.255.255.0
home-agent 43.0.0.3
```

Foreign Agent Example

The following example shows the foreign agent configuration:

```
!
interface Serial4/0
! Uplink interface
 ip address 11.0.0.2 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 5
 ip irdp holdtime 30
 ip mobile foreign-service
!
router mobile
!
ip mobile foreign-agent care-of Serial4/0 interface-only transmit-only
```

Additional References

For additional information related to the Cisco Mobile Networks—Asymmetric Link feature, refer to the following sections:

- Related Documents, page 10
- Standards, page 10
- MIBs, page 10
- RFCs, page 11
- Technical Assistance, page 11

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.
Cisco Mobile Networks commands	"Cisco Mobile Networks" feature document, Release 12.2(4)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 foreign-agent**
- **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 colocated 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.

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

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

satellite communications—The use of geostationary orbiting satellites to relay information.

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

Cisco Mobile Networks—Static Collocated Care-of Address

The Cisco Mobile Networks—Static Collocated Care-of Address feature allows a mobile router to roam to foreign networks where foreign agents are not deployed. Before the introduction of this feature, the mobile router was required to use a foreign agent care-of address when roaming. Now a roaming interface with a static IP address configured on the mobile router itself works as the collocated care-of address (CCoA).

Feature Specifications for Cisco Mobile Networks—Static Collocated Care-of Address

Feature History	
Release	**Modification**
12.2(15)T	This feature was introduced.
Supported Platforms	
For information about platforms supported, refer to Cisco Feature Navigator.	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Cisco Mobile Networks—Static CCoA

Static CCoA applies to networks where the endpoint IP address is always fixed, such as in a Cellular Digital Packet Data (CDPD) wireless network.

Restrictions for Cisco Mobile Networks—Static CCoA

Static CCoA is not recommended for environments where the endpoint IP address is not always fixed such as in the Dynamic Host Configuration Protocol (DHCP) or PPP/IPCP where the CCoA and gateway IP address are obtained dynamically.

Information About the Cisco Mobile Networks—Static CCoA

Before you configure static CCoA, you should understand the following concepts:

Care-of Addresses

If a mobile node or mobile router determines that it is connected to a foreign network, it acquires a care-of address. This care-of address is the exit-point of the tunnel towards the mobile node. 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. Two types of care-of addresses exist:

- Care-of address acquired from a foreign agent
- Collocated care-of address

A foreign agent care-of address is an IP address on a foreign agent that is advertised on the foreign network being visited by a mobile node. A mobile node that acquires this type of care-of address can share the address with other mobile nodes. A collocated care-of address is an IP address assigned to the interface of the mobile node itself. A collocated care-of address represents the current position of the mobile node on the foreign network and can be used by only one mobile node at a time.

For the Cisco Mobile Networks—Static CCoA feature, a static collocated care-of address is a fixed IP address configured on a roaming interface of the mobile router.

CCoA support using a dynamically acquired IP address will be available in a future release.

Benefits of Cisco Mobile Networks—Static CCoA

This feature allows a mobile router to roam to foreign networks where foreign agents are not deployed.

Feature Design of Cisco Mobile Networks—Static CCoA

In general, static CCoA is intended for links where there are no foreign agents. If foreign agents are present, the interface will not support foreign agent care-of address roaming while the interface is configured for static CCoA. Any foreign agent advertisements detected on that interface will be ignored. A static CCoA interface will solicit advertisements if configured but will not automatically solicit advertisements when the interface comes up. This behavior overrides the default behavior—typically, in the Cisco Mobile Networks feature, when an interface goes down and comes back up, foreign agent advertisements are solicited automatically.

When the mobile router registers a CCoA with a home agent, a single HA-CCoA tunnel is created and is used for traffic to the mobile router and its mobile networks.

The static CCoA configured on the mobile router interface will become the endpoint of the HA-CCoA tunnel as the home agent tunnels packets to the mobile router. The mobile router will use this same tunnel to reverse tunnel packets back to the home agent if configured.

How to Configure Cisco Mobile Networks—Static CCoA

This section contains the following procedures:

- Enabling Static CCoA Processing on a Mobile Router Interface
- Verifying the Static CCoA Configuration

Enabling Static CCoA Processing on a Mobile Router Interface

To enable static CCoA processing on a mobile router interface, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip mobile router-service roam**
6. **ip mobile router-service collocated** [**gateway** *ip-address*]
7. **ip mobile router-service collocated registration retry** *seconds*

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 1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.6.23 255.255.255.0`	Sets a primary IP address for an interface. • This is the static CCoA.
Step 5	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 6	**ip mobile router-service collocated** [**gateway** *ip-address*] **Example:** `Router(config-if)# ip mobile router-service collocated gateway 168.71.6.1`	Enables static CCoA processing on a mobile router. • The gateway IP address is the next hop IP address for the mobile router to forward packets. The gateway IP address is required only on Ethernet interfaces, and must be on the same logical subnet as the primary interface address specified in Step 4.
Step 7	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You only need to use this command when a different retry interval is desired.

Troubleshooting Tips

The gateway IP address required on Ethernet interfaces is the next-hop IP address, not the CCoA. The gateway IP address must be on the same logical subnet as the primary interface address.

Verifying the Static CCoA Configuration

To verify the static CCoA configuration, perform the following optional steps:

SUMMARY STEPS

1. **show ip mobile router interface**
2. **show ip mobile router agent**
3. **show ip mobile router registration**
4. **show ip mobile router**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip mobile router interface** **Example:** `Mobilerouter# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming. • If the interface is configured for CCoA, the CCoA (IP address) is displayed even if the interface is down.
Step 2	**show ip mobile router agent** **Example:** `Mobilerouter# show ip mobile router agent`	Displays information about the agents for the mobile router. • If the interface configured for CCoA is up, an entry is shown.
Step 3	**show ip mobile router registration** **Example:** `Mobilerouter# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 4	**show ip mobile router** **Example:** `Mobilerouter# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuration Examples for Cisco Mobile Networks—Static CCoA

This section provides the following configuration example:

- Mobile Networks with Static CCoA Example

Mobile Networks with Static CCoA Example

The following example shows a mobile router configured with a static CCoA address of 172.21.58.23 and a next-hop gateway address of 172.21.58.1.

```
interface loopback 0
! MR home address
 ip address 10.1.0.1 255.255.255.255
!
!Static CCoA
interface FastEthernet0/0
```

```
 ip address 172.21.58.23 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 172.21.58.1
 ip mobile router-service collocated registration retry 3
!
router mobile
!
ip mobile router
 address 10.1.0.1 255.255.255.255
 home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 100 key hex 12345678123456781234567812345678
```

Additional References

For additional information related to Cisco Mobile Networks—Static Collocated Care-of Address, see the following references:

- Related Documents
- Standards
- MIBs
- RFCs
- Technical Assistance

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
Mobile IP commands related to Cisco Mobile Networks	"Cisco Mobile Networks" feature document, Release 12.2(4)T and 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

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*.

- **collocated single-tunnel**
- **ip mobile router-service collocated**
- **ip mobile router-service collocated registration retry**
- **show ip mobile router**
- **show ip mobile router agent**
- **show ip mobile router interface**
- **show ip mobile router registration**

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.

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.

link—A facility or medium over which mobile nodes communicate at the link layer. A link underlies the network layer.

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

Cisco Mobile Networks—Priority HA Assignment

Before the introduction of the Cisco Mobile Networks—Priority HA Assignment feature, the mobile router preconfigured home agents (HAs) with different priorities, registering with only the highest priority home agent. However, a mobile router may roam to an area where registration with a closer home agent is more desirable. This feature allows a mobile router to register with the closer home agent using the combination of existing home agent priority configurations on the mobile router and care-of address access lists configured on the home agent.

Feature Specifications for the Cisco Mobile Networks—Priority HA Assignment Feature

Feature History	
Release	**Modification**
12.2(15)T	This feature was introduced.
Supported Platforms	
For information about platforms supported, refer to Cisco Feature Navigator.	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Cisco Mobile Networks—Priority HA Assignment

Before you configure the Cisco Mobile Networks—Priority HA Assignment feature, you should understand the following concepts:

- Feature Design of Cisco Mobile Networks—Priority HA Assignment, page 2
- Benefits of Cisco Mobile Networks—Priority HA Assignment, page 2

Feature Design of Cisco Mobile Networks—Priority HA Assignment

This feature changes the behavior of the HA priority configurations on the mobile router without adding any new commands. Each HA will have an access list containing all the foreign agent care-of addresses in its region. When a mobile router sends a registration request to the best HA, the HA will accept or deny the request depending on which care-of address is used in the registration request. If the HA denies the request because the care-of address is not in the access list of that particular HA, the mobile router will try to register with the next best HA, and so on. If HAs have the same priority, then the most recently configured HA takes precedence. If registration with even the lowest priority HA fails, the mobile router will wait for an advertisement and then try to register again starting with the highest priority HA. When the mobile router registers with a new HA, it will also attempt to deregister with the old HA using the old foreign agent care-of address.

Benefits of Cisco Mobile Networks—Priority HA Assignment

This feature allows a mobile router to register with a geographically closer HA, which improves latency on the network.

How to Configure Cisco Mobile Networks—Priority HA Assignment

This section includes the following procedures:

- Configuring Care-of Address Access Lists on an HA, page 2
- Configuring HA Priorities on the Mobile Router, page 6

Configuring Care-of Address Access Lists on an HA

This task describes how to configure care-of address access lists on an HA.

Best HA Selection Process

If more than one HA is reachable from any care-of address that may be used by the mobile router, then the HAs need an access list (which is a foreign agent care-of address or collocated care-of address) configured to enforce the best HA selection process. This configuration enforces a region covered by a specific HA defined by the care-of addresses (configured as access lists) within the region. Registrations originating outside the region are administratively denied while registrations within the region are processed.

Restrictions

Without the **distribute-list** command configured, each HA will advertise a route to the same virtual network. This situation may cause routing conflicts and traffic destined to the home network of the mobile router to be dropped.

With the **distribute-list** command configured, you can suppress the advertisement of the virtual networks to the rest of the network. However, pings to the mobile router home address will fail but pings to an address with the mobile network served by the mobile router will succeed. Traffic destined to the mobile network would continue to reach the destination without problems.

If the home network consists of both mobile routers and mobile nodes, the **distribute-list** command will block only the addresses of the mobile routers and not the entire subnet.

Routes to the mobile router are not advertised when the mobile router is not registered. Pings to an address on the mobile network will return unreachable if the mobile router is not registered.

Mobile networks will only be advertised by one HA at a time as long as deregistration to the old HA is successful. After roaming to a new HA, pings to the mobile network may take some time depending on how fast the mobile network route is propagated throughout the network by the routing protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile home-agent care-of-access** *access-list*
4. **ip access-list standard** *access-list-name*
5. **permit** *coa-ip-address*
6. **permit** *mr-home-address*
7. **exit**
8. **router** *protocol*
9. **redistribute mobile subnets**
10. **distribute-list** *access-list* **out**
11. **exit**
12. **access-list** *access-list-number* **deny** *source*
13. **access-list** *access-list-number* **permit any**
14. Repeat Steps 3 through 7 for each HA configured on the mobile router. Repeat Steps 8 through 13 for each HA if virtual networks are configured.

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 care-of-access** *access-list* **Example:** `Router(config)# ip mobile home-agent care-of-access HA1-FA1`	Controls which care-of addresses in registration requests are permitted by the home agent. • By default, all care-of addresses are permitted. The access list can be a string or number from 1 to 99.
Step 4	**ip access-list standard** *access-list-name* **Example:** `Router(config)# ip access-list standard HA1-FA1`	Defines a standard access list and enters standard named access list configuration mode. • Use this command to configure access lists on each HA that is reachable by the mobile router.
Step 5	**permit** *coa-ip-address* **Example:** `Router(config-std-nacl)# permit 3.3.3.2`	Sets conditions for an access list. • The *coa-ip-address* can be a foreign agent care-of address or a collocated care-of address. This command informs the HA which care-of addresses can be accepted in a registration request.
Step 6	**permit** *mr-home-address* **Example:** `Router(config-std-nacl)# permit 5.5.5.3`	Sets conditions for an access list. • The *mr-home-address* is the home address for the mobile router. See the "Troubleshooting Tips" section below for an explanation as to why it is important to include the mobile router home address.
Step 7	**exit** **Example:** `Router(config-std-nacl)# exit`	Exits to global configuration mode.
Step 8	**router** *protocol* **Example:** `Router(config)# router ospf`	Configures a routing protocol.
Step 9	**redistribute mobile subnets** **Example:** `Router(config-router)# redistribute mobile subnets`	Enables redistribution of a virtual network into routing protocols.

	Command or Action	Purpose
Step 10	**distribute-list** *access-list* **out** **Example:** `Router(config-router)# distribute-list 1 out`	(Optional) Suppresses networks from being advertised in updates. • This command configured on each HA will prevent the advertisement of the virtual network for the mobile routers. See the "Restrictions" and "Troubleshooting Tips" sections for more information about using this command.
Step 11	**exit** **Example:** `Router(config-router)# exit`	Exits to global configuration mode.
Step 12	**access-list** *access-list-number* **deny** *source* **Example:** `Router(config)# access-list 1 deny 5.5.5.0`	Defines a standard IP access list. • Denies access if the conditions are matched. • In this example, the *source* value is the the virtual network configured on the HA. The **distribute-list** command in Step 10 prevents the advertisement of this virtual network.
Step 13	**access-list** *access-list-number* **permit any** **Example:** `Router(config)# access-list 1 permit any`	Defines a standard IP access list. • Permits access if the conditions are matched.
Step 14	Repeat Steps 3 through 7 for each HA configured on the mobile router. Repeat Steps 8 through 13 for each HA if virtual networks are configured.	—

Troubleshooting Tips

Care-of Address List Operation

Any time an HA has a care-of address access list configured, the access list should permit the mobile router home address (for deregistration) and the interesting list of care-of addresses (for registration).

The care-of address lists are designed to allow registrations only of a select group of care-of addresses on an HA. For priority HA assignment to work, deregistrations need to be allowed as well. The deregistration is sent with the mobile router home address in the care-of address field of the deregistration. If the home address is not permitted, any deregistration will be dropped by the access list. Priority HA assignment does not work properly if the deregistrations are dropped.

Virtual Network Advertisements

In a network using mobile routers configured with priority HA assignment and multiple HAs, the HAs may be sharing routing information. If so, each HA will advertise a route to the same mobile virtual network through the **redistribute mobile** command. This situaton results in multiple routes to the same virtual network, which can cause routing conflicts and lost packets. The **distribute-list** command configured on each HA will prevent the advertisement of the virtual-network for the mobile routers. There is no dependency on registration for this to occur.

Configuring HA Priorities on the Mobile Router

This task describes how to configure HA priorities on the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile router**
4. **home-agent** *ip-address* **priority** *level*
5. **end**
6. **show ip mobile router**

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 router`** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 4	**`home-agent`** *`ip-address`* **`priority`** *`level`* **Example:** `Router(mobile-router)# home-agent 1.1.1.1 priority 101`	Specifies the home agent that the mobile router uses during registration. • The priority level prioritizes which home agent address is the best to use during registration. The range is from 0 to 255, where 0 denotes the lowest priority and 255 denotes the highest priority. The default is 100.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(mobile-router)# end`	Exits to privileged EXEC mode.
Step 6	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router. • This command displays the home agent that the mobile router is registered with. The qualifiers (best) (current) displayed after the home agent entry indicates that this home agent was chosen as the best home agent to register with. See the display output in the "Examples" section.

Examples

This section provides the following output example for the **show ip mobile router** command:

The following example shows that the mobile router is currently registered with the best home agent located at 200.200.200.1:

```
Router# show ip mobile router

Mobile Router
  Enabled 01/01/02 10:01:34
  Last redundancy state transition NEVER

Configuration:
  Home Address 5.5.5.3 Mask 255.255.255.0
  Home Agent 200.200.200.1 Priority 102 (best) (current)
        100.100.100.1 Priority 101
  Registration lifetime 90 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Extend Expire 120, Retry 3, Interval 10

Monitor:
  Status -Registered-
  Active foreign agent 3.3.3.2, Care-of 3.3.3.2
  On interface Ethernet5/3
```

Configuration Examples for Cisco Mobile Networks—Priority HA Assignment

This section provides the following configuration example:

- HA Priority Configuration Example, page 7

HA Priority Configuration Example

In the following example, two home agents are configured with access lists that allow the mobile router to choose the best HA to register with:

Home Agent1

```
interface Loopback0
 ip address 100.100.100.1 255.255.255.255
!
interface Ethernet1
 ip address 2.2.2.1 255.255.255.0
!
router mobile
!
router ospf 100
 redistribute mobile subnets
 network 2.0.0.0 0.255.255.255 area 0
 network 100.100.100.0 0.255.255.255 area 0
! Suppresses virtual network to be advertised in updates
 distribute-list 1 out
!
ip mobile home-agent care-of-access HA1-FA1
ip mobile virtual-network 5.5.5.0 255.255.255.0
ip mobile host 5.5.5.3 virtual-network 5.5.5.0 255.255.255.0 lifetime 90
ip mobile mobile-networks 5.5.5.3
 description Jet
 network 6.6.6.0 255.255.255.0
ip mobile secure host 5.5.5.3 spi 100 key hex 12345678123456781234567812345678 algorithm
md5 mode prefix-suffix
!
ip access-list standard HA1-FA1
! MR CCOA
 permit 4.4.4.2
! FA1 COA
 permit 7.7.7.1
! MR home address
 permit 5.5.5.3
!
! Denies virtual network to
access-list 1 deny 5.5.5.0 0.0.0.255
access-list 1 permit any
```

Home Agent 2

```
interface Loopback0
 ip address 200.200.200.1 255.255.255.255
!
interface Ethernet0
 ip address 1.1.1.1 255.255.255.0
!
router mobile
!
router ospf 100
 redistribute mobile subnets
 network 1.0.0.0 0.255.255.255 area 0
 network 200.200.200.0 0.255.255.255 area 0
! Suppresses virtual network to be advertised in update
 distribute-list 1 out
!
ip mobile home-agent care-of-access HA2-FA2
ip mobile virtual-network 5.5.5.0 255.255.255.0
ip mobile host 5.5.5.3 virtual-network 5.5.5.0 255.255.255.0 lifetime 90
ip mobile mobile-networks 5.5.5.3
 description Jet
 network 6.6.6.0 255.255.255.0
ip mobile secure host 5.5.5.3 spi 200 key hex 12345678123456781234567812345678 algorithm
md5 mode prefix-suffix
!
```

```
ip access-list standard HA2-FA2
! FA COA
 permit 3.3.3.2
! MR home address
 permit 5.5.5.3
!
access-list 1 deny 5.5.5.0 0.0.0.255
access-list 1 permit any
```

Mobile Router

```
interface Loopback0
 ip address 5.5.5.3 255.255.255.255
!
! CCOA roaming interface registers with HA1 only
interface Ethernet5/1
 ip address 4.4.4.3 255.255.255.0
 ip mobile router-service roam priority 99
 ip mobile router-service collocated gateway 4.4.4.2
!
! This roaming interface will use FA COA to register
interface Ethernet5/3
 ip address 3.3.3.3 255.255.255.0
 ip mobile router-service roam
!
! Mobile Network interface
interface Ethernet5/4
 ip address 6.6.6.3 255.255.255.0
!
router mobile
!
ip mobile secure home-agent 100.100.100.1 spi 100 key hex 12345678123456781234567812345678
algorithm md5 mode prefix-suffix
ip mobile secure home-agent 200.200.200.1 spi 200 key hex 12345678123456781234567812345678
algorithm md5 mode prefix-suffix
!
ip mobile router
 address 5.5.5.3 255.255.255.0
 home-agent 100.100.100.1 priority 101
 home-agent 200.200.200.1 priority 102
 register lifetime 90
```

Additional References

For additional information related to the Cisco Mobile Networks—Priority HA Assignment feature, see to the following sections:

- Related Documents
- Standards
- MIBs
- RFCs
- Technical Assistance

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 T
Mobile IP commands related to Cisco mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 12.2(13)T
Access list commands	*"IP Services Commands"* chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 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

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

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.

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*.

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.

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, or bicycle. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

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

Cisco Mobile Networks—Tunnel Templates for Multicast

The Cisco Mobile Networks—Tunnel Templates for Multicast feature allows the configuration of multicast on statically created tunnels to be applied to dynamic tunnels brought up on the home agent and mobile router. A tunnel template is defined and applied to the tunnels between the home agent and mobile router. The mobile router can now roam and the tunnel template enables multicast sessions to be carried to the mobile networks.

Feature Specifications for Cisco Mobile Networks—Tunnel Templates for Multicast

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

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Glossary, page 9

Prerequisites for Cisco Mobile Networks—Tunnel Templates for Multicast

Reverse tunneling must be enabled from the mobile router to the home agent.

Restrictions for Cisco Mobile Networks—Tunnel Templates for Multicast

Tunnels cannot be removed if they are being used as templates.

How to Configure Tunnel Templates for Multicast

This section contains the following procedures:

- Applying the Tunnel Template on the Home Agent (required)
- Applying the Tunnel Template on the Mobile Router (required)

Applying the Tunnel Template on the Home Agent

This task describes how to apply the tunnel template to the tunnels brought up at the home agent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **interface tunnel** *interface-number*
5. **ip pim sparse-mode**
6. **exit**
7. **router mobile**
8. **exit**
9. **ip mobile mobile-networks**
10. **template tunnel** *interface-number*
11. **end**
12. **show ip mobile tunnel**

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 multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**interface tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 100`	Designates a tunnel interface and enters interface configuration mode. • This is the tunnel template that will be applied to the mobile networks.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on the tunnel interface in sparse mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 8	**exit** **Example:** `Router(config-router)#` **exit**	Returns to global configuration mode.
Step 9	**ip mobile mobile-networks** **Example:** `Router(config)# ip mobile mobile-networks`	Configures mobile networks for the mobile host and enters mobile networks configuration mode.
Step 10	**template tunnel** *interface-number* **Example:** `Router(mobile-networks)# template tunnel 100`	Designates the tunnel template to apply during registration. • The *interface-number* argument is set to the tunnel template defined in Step 4.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(mobile-networks)# end`	Exits to privileged EXEC mode.
Step 12	**show ip mobile tunnel** **Example:** `Router# show ip mobile tunnel`	Displays active tunnels. • Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example displays the active Mobile IP tunnels and the template configuration for the tunnel on the home agent:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Total mobile ip tunnels 2
Tunnel1:
    src 1.1.1.1, dest 20.20.0.1
    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 Tunnel0
    HA created, fast switching enabled, ICMP unreachable enabled
    27 packets input, 2919 bytes, 0 drops
    24 packets output, 2568 bytes
Running template configuration for this tunnel:
ip pim sparse-dense-mode

Tunnel0:
    src 1.1.1.1, dest 30.30.10.2
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Ethernet1/3
    HA created, fast switching enabled, ICMP unreachable enabled
    0 packets input, 0 bytes, 0 drops
    24 packets output, 3048 bytes
```

Applying the Tunnel Template on the Mobile Router

This task describes how to apply the tunnel template to the tunnels brought up at the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **interface tunnel** *interface-number*
5. **ip pim sparse-mode**

6. **exit**
7. **router mobile**
8. **exit**
9. **ip mobile router**
10. **template tunnel** *interface-number*
11. **end**
12. **show ip mobile tunnel**

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 multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**interface tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 100`	Designates a tunnel interface and enters interface configuration mode. • This is the tunnel template that will be applied to the mobile networks.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on the tunnel interface in sparse mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 8	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 9	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 10	**template tunnel** *interface-number* **Example:** `Router(mobile-router)# template tunnel 100`	Designates the tunnel template to apply during registration. • The *interface number* argument is set to the tunnel template defined in Step 4.
Step 11	**end** **Example:** `Router(mobile-router)# end`	Exits to privileged EXEC mode.
Step 12	**show ip mobile tunnel** **Example:** `Router# show ip mobile tunnel`	Displays active tunnels. • Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example displays the active Mobile IP tunnels and the template configuration for the tunnel on the mobile router:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 20.20.0.1, dest 1.1.1.1
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Ethernet4/2
    MR created, fast switching enabled, ICMP unreachable enabled
    22 packets input, 2468 bytes, 0 drops
    27 packets output, 2892 bytes
Running template configuration for this tunnel:
ip pim sparse-mode
```

Configuration Examples for Tunnel Templates for Multicast

This section provides the following configuration example:

- Tunnel Templates for Multicast Example, page 7

Tunnel Templates for Multicast Example

In the following example, a tunnel template is defined and configured to be brought up at the home agent and mobile router. The foreign agent does not require any additional configuration to support the Cisco Mobile Networks—Tunnel Templates for Multicast feature.

Home Agent Configuration

```
!
ip multicast-routing
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
!
! Tunnel template to be applied to mobile networks
interface tunnel100
 ip address 13.0.0.1 255.0.0.0
 ip pim sparse-mode
!
!
router mobile
ip mobile mobile-networks 11.1.0.1
 description jet
 network 11.1.2.0 255.255.255.0
 network 11.1.1.0 255.255.255.0
! Select tunnel template to apply during registration
 template tunnel100
!
ip mobile secure host 11.1.0.1 spi 101 key hex 12345678123456781234567812345678 algorithm
md5 mode prefix-suffix
!
no ip mobile tunnel route-cache
!
```

Mobile Router Configuration

```
!
ip multicast-routing
!
interface Loopback0
 ip address 11.1.0.1 255.255.255.255
 ip pim sparse-mode
!
!
! Tunnel template to be applied to mobile networks
interface tunnel 100
 no ip address
 ip pim sparse-mode
!
!
interface Ethernet1/1
 ip address 20.0.0.1 255.0.0.0
 ip pim sparse-mode
 ip mobile router-service roam
!
router mobile
ip pim rp-address 7.7.7.7
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781
algorithm md5 mode prefix-suffix
ip mobile router
```

```
 address 11.2.0.1 255.255.0.0
 home-agent 1.1.1.1
! Select tunnel template to apply during registration
 template tunnel 100
 register extend expire 5 retry 2 interval 15
 register lifetime 10000
 reverse-tunnel
!
```

Additional References

For additional information related to Cisco Mobile Networks—Tunnel Templates for Multicast, see the following sections:

- Related Documents
- Standards
- MIBs
- RFCs
- Technical Assistance

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 Comman ds" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2
Multicast configuration tasks	"Configuring IP Multicast Routing" chapter in the *Cisco IOS IP Configuration Guide,* Release 12.2
Multicast commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"IP Multicast Routing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast,* Release 12.2
Mobile IP commands related to Cisco Mobile Networks	*Cisco Mobile Networks* feature document, Releases 12.2(4)T and 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
None	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

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*.

- **show ip mobile tunnel**
- **template tunnel (mobile networks)**
- **template tunnel (mobile router)**

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*.

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

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

Mobile Networks Dynamic Collocated Care-of Address

Before the introduction of the Mobile Networks Dynamic Collocated Care-of Address feature, Cisco mobile networks supported foreign agent care-of address (CoA) registration and static collocated care-of address (CCoA) registration.

Static CCoA registration is considered a special case and applies to networks where the endpoint IP address is always fixed, such as in a Cellular Digital Packet Data (CDPD) wireless network. The Mobile Networks Static Collocated Care-of Address feature allows a mobile router with a static IP address to roam to foreign networks where foreign agents are not deployed.

The Mobile Networks Dynamic Care-of Address feature allows the mobile router to register with the home agent using a CCoA that is acquired dynamically via the IP Control Protocol (IPCP). Support for CCoAs acquired through the Dynamic Host Configuration Protocol (DHCP) is planned for a future release.

Feature History for the Mobile Networks Dynamic Collocated Care-of Address Feature

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

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Mobile Networks Dynamic CCoA

The Mobile Networks Dynamic CCoA feature can be configured only on serial (point-to-point) interfaces.

Information About Mobile Networks Dynamic CCoA

Before you configure the Mobile Networks Dynamic CCoA feature, you should understand the following concepts:

Care-of Addresses

If a mobile router determines that it is connected to a foreign network, it acquires a care-of address. This care-of address is the exit point of the tunnel from the home agent toward the 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 router in its current location. There are two types of care-of addresses:

- Care-of address acquired from a foreign agent
- Collocated care-of address

A foreign agent care-of address is an IP address on a foreign agent that is advertised on the foreign network being visited by a mobile router. A foreign agent CoA can be shared by other mobile routers. A collocated care-of address is an IP address assigned to the interface of the mobile router itself. A collocated care-of address represents the current position of the mobile router on the foreign network and can be used by only one mobile router at a time.

Mobile Networks Dynamic CCoA Feature Design

The Mobile Networks Dynamic CCoA feature is very similar to the static CCoA implementation. Static CCoA uses the address configured on the roaming interface as the CCoA. Dynamic CCoA uses IPCP to obtain a CCoA for the roaming interface. See the *Cisco Mobile Networks - Static Collocated Care-of Address* feature documentation for more information on the static CCoA implementation.

For both static and dynamic CCoA, the interface can be configured to exclusively use CCoAs for registration or to use a foreign agent CoA if one is available. In the foreign agent case, when an interface first comes up, it will attempt to discover foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile router will register using the advertised CoA. The interface will continue to register using a CoA as long as a foreign agent is heard. When foreign agents are not heard, either because no advertisements are received or the foreign agent advertisement hold time expires, CCoA processing is enabled and the interface registers its CCoA. The CCoA is the interface's statically configured or dynamically acquired primary IP address. If a foreign agent is heard again, the interface will again register the foreign agent CoA.

You can configure the interface to register only its CCoA and ignore foreign agent advertisements by using the **ip mobile router-service collocated ccoa-only** option.

When the mobile router registers a CCoA with a home agent, a single HA-CCoA tunnel is created and is used for traffic to the mobile router and its mobile networks.

The CCoA configured on the mobile router interface will become the endpoint of the HA-CCoA tunnel as the home agent tunnels packets to the mobile router. The mobile router will use this same tunnel to reverse tunnel packets back to the home agent if configured for reverse tunnel.

Benefits of Mobile Networks Dynamic CCoA

This feature allows a mobile router to roam to foreign networks where foreign agents are not deployed and to obtain a CCoA dynamically through IPCP.

How to Configure Mobile Networks Dynamic CCoA

This section contains the following procedures:

- Enabling Dynamic CCoA Processing on a Mobile Router Interface, page 3 (required)
- Enabling CCoA-Only Processing on a Mobile Router Interface, page 4 (optional)
- Verifying the Dynamic CCoA Configuration, page 6 (optional)

Enabling Dynamic CCoA Processing on a Mobile Router Interface

This task shows how to enable dynamic CCoA processing on a mobile router interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address negotiated**
5. **encapsulation ppp**
6. **ip mobile router-service roam**
7. **ip mobile router-service collocated**
8. **ip mobile router-service collocated registration retry** *seconds*

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 serial 1`	Configures an interface type and enters interface configuration mode. • Dynamic CCoAs can be acquired only on serial interfaces.
Step 4	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is obtained via IPCP address negotiation.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP enacapsulation on a specified serial interface.
Step 6	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 7	**ip mobile router-service collocated** **Example:** `Router(config-if)# ip mobile router-service collocated`	Enables CCoA processing on a mobile router interface. • The interface will first solicit foreign agent advertisements and register with a foreign agent CoA if an advertisement is heard. If no advertisements are received, CCoA registration is attempted.
Step 8	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You need to use this command only when a different retry interval is desired.

Enabling CCoA-Only Processing on a Mobile Router Interface

Perform this task to configure a mobile router interface to ignore foreign agent advertisements and exclusively use CCoAs for registration to the home agent. This functionality works for both static and dynamic CCoA processing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
   or
   ip address negotiated
5. **ip mobile router-service roam**
6. **ip mobile router-service collocated ccoa-only**
7. **ip mobile router-service collocated gateway** *ip-address* **ccoa-only**
8. **ip mobile router-service collocated registration retry** *seconds*

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 1`	Configures an interface type and enters interface configuration mode.

Step 4	**ip address** *ip-address mask*
	
	or
	
	ip address negotiated
	
	Example:
	`Router(config-if)# ip-address 172.71.6.23 255.255.255.0`
	
	or
	
	`Router(config-if)# ip address negotiated`
		Sets a primary IP address for an interface.
		• This is the static CCoA. Static CCoAs can be configured on serial or Ethernet interfaces.
		
		or
		
		Specifies that the IP address for a particular interface is obtained via IPCP address negotiation.
		• Use this command for dynamic CCoA processing. Dynamic CCoAs can be acquired only on serial interfaces.

Step 5	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.

	Command or Action	Purpose
Step 6	**ip mobile router-service collocated ccoa-only** **Example:** `Router(config-if)# ip mobile router-service collocated ccoa-only`	Enables CCoA-only processing on a mobile router interface. • This command can be used on serial interfaces for dynamic or static CCoA processing. • This command disables foreign-agent CoA processing and limits the interface to CCoA processing only. • If you use this command on an interface already registered with a foreign agent CoA, the mobile router will re-register immediately with a CCoA.
Step 7	**ip mobile router-service collocated gateway** *ip-address* **ccoa-only** **Example:** `Router(config-if)# ip mobile router-service collocated gateway 10.21.0.2 ccoa-only`	(Optional) Enables CCoA-only processing on a mobile router interface. • This command can be used only on Ethernet interfaces for static CCoA processing. • The gateway IP address is the next hop IP address for the mobile router to forward packets. The gateway IP address is required only on Ethernet interfaces, and must be on the same logical subnet as the primary interface.
Step 8	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You need to use this command only when a different retry interval is desired.

Verifying the Dynamic CCoA Configuration

Perform this task to verify the dynamic CCoA configuration:

SUMMARY STEPS

1. **show ip mobile router interface**
2. **show ip mobile router agent**
3. **show ip mobile router registration**
4. **show ip mobile router**
5. **show ip mobile binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip mobile router interface** **Example:** `Mobilerouter# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming. • If the interface is configured for CCoA, the CCoA (IP address) is displayed even if the interface is down.
Step 2	**show ip mobile router agent** **Example:** `Mobilerouter# show ip mobile router agent`	Displays information about the agents for the mobile router. • If the interface configured for CCoA is up, an entry is shown.
Step 3	**show ip mobile router registration** **Example:** `Mobilerouter# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 4	**show ip mobile router** **Example:** `Mobilerouter# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
Step 5	**show ip mobile binding** **Example:** `Homeagent# show ip mobile router`	Displays the mobility binding table. • If a CCoA is registered with the home agent, (D) direct-to-mobile node is displayed in the Routing Options field.

Configuration Examples for Mobile Networks Dynamic CCoA

This section provides the following configuration example:

- Mobile Networks Dynamic CCoA: Example, page 7
- Mobile Networks with CCoA-Only Processing: Example, page 8

Mobile Networks Dynamic CCoA: Example

The following example shows a mobile router configured to obtain a CCoA dynamically through IPCP:

```
interface loopback 0
! MR home address
 ip address 10.1.0.1 255.255.255.255
!
! Dynamic CCoA.
interface Serial 3/1
 ip address negotiated
 encapsulation ppp
 ip mobile router-service roam
 ip mobile router-service collocated
```

Mobile Networks with CCoA-Only Processing: Example

The following example shows a mobile router configured to obtain a static CCoA only. The interface will not listen to foreign agent advertisements.

```
interface loopback1
 ip address 20.0.4.1 255.255.255.255
!
! Static CCoA with CCoA-only option
interface Ethernet 1/0
 ip address 10.0.1.1 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 10.0.1.2 ccoa-only
 ip mobile router-service collocated registration retry 30
```

The following example shows a mobile router configured to obtain a dynamic CCoA only. The interface will not listen to foreign agent advertisements.

```
interface loopback1
 ip address 20.0.4.1 255.255.255.255
!
! Dynamic CCoA with CCoA-only option
interface Serial 2/0
 ip address negotiated
 encapsulation ppp
 ip mobile router-service roam
 ip mobile router-service collocated ccoa-only
 ip mobile router-service collocated registration retry 30
```

Additional References

The following sections provide additional references related to the Mobile Networks Dynamic CCoA 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
Mobile IP commands and configuration tasks related to mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 12.2(13)T
Static CCoA documentation	*Cisco Mobile Networks - Static Collocated Care-of Address*, Release 12.2(15)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 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*.

- **ip mobile router-service collocated**
- **show ip mobile router agent**
- **show ip mobile router interface**

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.

collocated care-of address—The termination point of a tunnel toward a mobile node or mobile router. A CCoA is a local address that the mobile node or mobile router associated with one of its own network interfaces.

foreign agent—A router on the visited network of a foreign network that provides routing services to the mobile node or mobile router 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.

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

Mobile Networks Deployment MIB

The Mobile Networks Deployment MIB feature provides MIB support for customers deploying Cisco Mobile Networks functionality. Mobile IP management using Simple Network Management Protocol (SNMP) is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB.

This feature is useful for customers deploying mobile networks functionality that need to monitor and debug mobile router information via SNMP.

Feature History for the Mobile Networks Deployment MIB Feature

Release	Modification
12.3(4)T	This feature was introduced.
12.3(11)T	Support for the Cisco 3200 platform was added.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Additional References

The following sections provide references related to the Mobile Networks Deployment MIB feature.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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
Mobile IP commands and configuration tasks related to mobile networks	*Cisco Mobile Networks,* Cisco IOS Release 12.2(4)T and Release 12.2(13)T
Cisco configuration fundamentals and network management commands	*Cisco IOS Configuration Fundamentals and Network Management Command Reference,* Release 12.3 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 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 mib**

Mobile IP - Foreign Agent Local Routing to Mobile Networks

In previous releases of Cisco IOS software, traffic from a correspondent node to a mobile router must always go through the mobile router's home agent (HA). The Mobile IP - Foreign Agent Local Routing to Mobile Networks feature allows traffic from local devices attached to the foreign agent (FA) to be routed directly through the FA to the mobile networks of mobile routers that are visiting the FA's subnets. Direct routing is accomplished by injecting routes to the mobile network into the routing table of the FA.

The Mobile IP - Foreign Agent Local Routing to Mobile Networks feature is useful in scenarios in which a mobile router needs to receive high bandwidth traffic, such as streaming video, from a device on the local LAN of the FA. This feature can also be useful any time that the bandwidth between the FA and the HA is limited.

Feature History for Mobile IP - Foreign Agent Local Routing to Mobile Networks Feature

Release	Modification
12.3(7)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Foreign Agent Local Routing to Mobile Networks

Modifications to the home agent were made to support foreign agent local routing. You must be running Cisco IOS Release 12.3(7)T or higher for both the home agent and foreign agent for this feature to function properly.

Restrictions for Foreign Agent Local Routing to Mobile Networks

- A security association between the home agent (HA) and the foreign agent (FA) is mandatory. FA local routing will not occur if there is no security association configured.
- Redistributing FA-injected routes thorough Interior Gateway Protocol (IGP) is not supported.
- The overlapping of mobile networks on the FA is not supported.

Information About Foreign Agent Local Routing to Mobile Networks

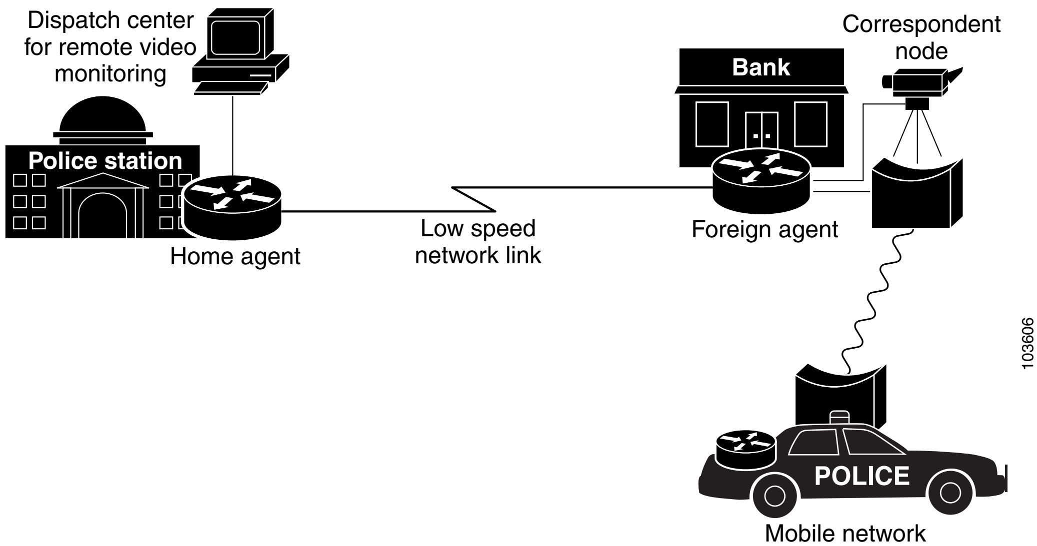
To configure the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature, you should understand the following concepts:

Foreign Agent Local Routing to Mobile Networks Feature Design

The Mobile IP - Foreign Agent Local Routing to Mobile Networks feature allows traffic from a correspondent node on a local subnet to route directly through the foreign agent (FA) to a mobile network that is visiting the FA. This direct routing is accomplished by injecting mobile network routes into the routing table of the FA.

This feature is useful in scenarios in which a mobile router needs to receive high bandwidth traffic, such as streaming video, from a device on the local LAN of the FA. An example of such a scenario is diagrammed in Figure 1.

Figure 1 Usage Scenario for the Mobile IP - Foreign Agent Local Routing to Mobile Networks Feature



In this scenario, a police officer has been called to a bank where an incident is occurring. The mobile router in the police officer's car registers with the FA and connects to the video streaming server, a correspondent node, that is located inside the bank. The police officer may then watch live video of the incident that is occurring inside the bank, gaining valuable information about how to proceed with handling the incident safely.

Before the introduction of the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature, the streaming video from the correspondent node in the bank would be routed from the FA to the HA, then back to the FA, and finally to the mobile router. This behavior, known as triangular routing, is not desirable for latency-sensitive applications. If a second police car arrived and wanted to watch the video as well, the already limited bandwidth between the FA and the HA would be even further taxed. The Mobile IP - Foreign Agent Local Routing to Mobile Networks feature allows traffic from the local corresponding node to be routed directly from the FA to the mobile router, eliminating the unnecessary trip to the HA.

Benefits of Foreign Agent Local Routing to Mobile Networks

The Mobile IP - Foreign Agent Local Routing to Mobile Networks feature improves latency by allowing the FA to route traffic directly to mobile networks rather than routing through the HA. This feature is useful in scenarios in which a mobile router needs to receive high bandwidth traffic, such as streaming video, from a device on the local LAN of the FA. This feature can also be useful any time that the bandwidth between the FA and the HA is limited.

How to Configure Foreign Agent Local Routing to Mobile Networks

This following sections describe configuration tasks for the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature:

- Configuring Local Routing to Mobile Networks on the Foreign Agent, page 4 (required)
- Configuring an Access List, page 5 (optional)

Configuring Local Routing to Mobile Networks on the Foreign Agent

This task describes how to configure the foreign agent for the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile foreign-agent inject-mobile-networks** [**mobnetacl** *access-list-identifier*]
4. **ip mobile secure** {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*]] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

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	**ip mobile foreign-agent inject-mobile-networks** [**mobnetacl** *access-list-identifier*] **Example:** `Router(config)# ip mobile foreign-agent inject-mobile-networks mobnetacl mobile-net-list`	Enables direct routing to the mobile networks via the foreign agent.
Step 4	**ip mobile secure** {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*]] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}] **Example:** `Router(config)# ip mobile secure home-agent 10.10.10.1 spi 1400 key hex 12345678123456781234567812345678 algorithm hmac-md5`	Specifies the mobility security associations for the mobile host, visitor, home agent, and foreign agent.

Troubleshooting Tips

Modifications to the home agent were made to support foreign agent local routing. You must be running Cisco IOS Release 12.3(7)T or higher for both the home agent and foreign agent for this feature to function properly. If the home agent version is lower than that, the foreign agent will report the following debug output from the **debug ip mobile** command:

```
*Jan 13 21:30:38.283: MobileIP: Parsing Dynamic Mobile Networks extension for MR10.2.2.2
*Jan 13 21:30:38.283: MobileIP: Parsed Mobile Network 0.0.0.0:0.0.0.0 for MR 10.2.2.2
```

You can recognize this problem by observing that the debug output on the foreign agent only indicates the single network of 0.0.0.0 0.0.0.0.

Configuring an Access List

To restrict which mobile networks will have their local routes injected into the FA routing table, you may choose to configure an access list. You can configure either a named access list or a numbered access list. Perform one of the following tasks to configure an access list on the FA:

- Configuring a Named Access List, page 5
- Configuring a Numbered Access List, page 6

Configuring a Named Access List

Perform this task to configure a named access list on the FA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit** *source* [*source-wildcard*]

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 access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list standard mobile-net-list`	Defines an IP access list by name.
Step 4	[*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `Router(config-std-nacl)# permit any`	Sets conditions to allow a packet to pass a named IP access list.

Configuring a Numbered Access List

Perform this task to configure a numbered access list on the FA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]

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	**`access-list`** *`access-list-number`* `{`**`deny`** `|` **`permit`**`}` *`source`* `[`*`source-wildcard`*`] [`**`log`**`]` **Example:** `Router(config)# access-list 88 permit any`	Defines a standard IP access list.

Configuration Examples for Foreign Agent Local Routing to Mobile Networks

The following sections contain configuration examples for the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature:

- Foreign Agent Local Routing to Mobile Networks Using a Named Access List: Example, page 7
- Foreign Agent Local Routing to Mobile Networks Using a Numbered Access List: Example, page 8

Foreign Agent Local Routing to Mobile Networks Using a Named Access List: Example

The following example configures the FA for local routing and uses a named access list:

```
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent inject-mobile-networks mobnetacl mobile-net-list
ip mobile foreign-agent reg-wait 120
ip mobile secure home-agent 10.10.10.1 spi 1400 key hex 12345678123456781234567812345678
     algorithm hmac-md5
!
ip access-list standard mobile-net-list
 permit any
```

Foreign Agent Local Routing to Mobile Networks Using a Numbered Access List: Example

The following example configures the FA for local routing and uses a numbered access list:

```
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent inject-mobile-networks mobnetacl 88
ip mobile foreign-agent reg-wait 120
ip mobile secure home-agent 10.10.10.1 spi 1400 key hex 12345678123456781234567812345678
     algorithm hmac-md5
!
access-list 88 permit any
```

Additional References

The following sections provide references related to the Mobile IP - Foreign Agent Local Routing to Mobile Networks 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
Mobile IP commands and configuration tasks related to mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 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 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*.

- **ip mobile foreign-agent inject-mobile-networks**
- **show ip mobile globals**

Glossary

correspondent node—A peer with which a mobile node or mobile router is communicating. A correspondent node may be either stationary or mobile.

foreign agent—A router on the visited 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 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 network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

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.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

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

Mobile IP - Generic Routing Encapsulation for Cisco Mobile Networks

Prior to the introduction of the Generic Routing Encapsulation for Cisco Mobile Networks feature, Cisco Mobile Networks supported only IP-in-IP encapsulation. This feature adds generic routing encapsulation (GRE) support for mobile networks. Benefits of the Generic Routing Encapsulation for Cisco Mobile Networks feature include the following:

- GRE supports multiprotocol tunneling.
- GRE provides explicit protection against recursive encapsulation.
- Hardware support of GRE tunneling increases the performance of the router.
- GRE keepalive messages allow the status of the end-to-end tunnel to be monitored.

Feature History for the Mobile IP - GRE for Cisco Mobile Networks Feature

Release	Modification
12.3(7)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for GRE for Cisco Mobile Networks

Roaming must be enabled on an interface before GRE encapsulation can be enabled on the interface.

Restrictions for GRE for Cisco Mobile Networks

The foreign agent (FA) and home agent (HA) must support GRE encapsulation in order for the mobile router to register with GRE encapsulation enabled. If the mobile router is attempting to register using collocated care-of address (CCoA) with GRE encapsulation, the HA must support GRE encapsulation.

GRE keepalives do not support Network Address Translation (NAT). If there is NAT in the path between a mobile router and its HA, GRE keepalive messages will not work properly. To work around the problem, consider using the Mobile IP NAT Traversal feature, which offers UDP encapsulation. The Mobile IP NAT Traversal feature documentation can be found at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gtnatmip.htm

Information About GRE for Cisco Mobile Networks

To configure the GRE for Cisco Mobile Networks feature, you should understand the following concepts:

Generic Routing Encapsulation

Generic routing encapsulation (GRE) is a tunneling protocol used by Mobile IP. The GRE tunnel interface creates a virtual point-to-point link between two routers at remote points over an IP internetwork. GRE tunnels can transport a passenger protocol or encapsulated protocol.

Unlike IP-in-IP encapsulation, GRE provides the following:

- Explicit protection against recursive encapsulation, a condition in which tunneled packets reenter the same tunnel before exiting.
- Configurable keepalive messages to monitor the end-to-end status of the tunnel.

GRE is beneficial for certain applications because of its support for multiprotocol tunneling and explicit prevention of recursive encapsulation.

GRE for Cisco Mobile Networks Feature Design

To understand the components of the Cisco Mobile Networks solution, refer to the *Cisco Mobile Networks* feature documentation.

During agent discovery, HAs and FAs advertise their presence on their attached links by periodically multicasting or broadcasting messages called agent advertisements. The agent advertisements are ICMP Router Discovery Protocol (IRDP) messages with one or more extensions specific to Mobile IP. The agent advertisement extension consists of several fields including the following field that is relevant to this feature:

- G: This agent can receive tunneled IP datagrams that use GRE (referred to as the G bit)

If the GRE for Cisco Mobile Networks feature is enabled, the mobile router will request GRE encapsulation in the registration request only if the FA advertises that it is capable of GRE encapsulation (the G bit is set in the advertisement). If the registration request is successful, packets will be tunneled using GRE encapsulation.

If the GRE for Cisco Mobile Networks feature is enabled and the mobile router is using collocated care-of address (CCoA), the mobile router will attempt to register with the HA using GRE encapsulation. If the registration request is successful, packets will be tunneled using GRE encapsulation.

If the mobile router receives a denied registration reply with error code 72 (foreign agent required encapsulation unavailable) or error code 139 (home agent unsupported encapsulation), the mobile router will send another registration request with the G bit unset and the default IP-in-IP encapsulation will be used.

GRE Keepalive Messages

GRE tunnels support keepalive messages, which are messages sent periodically to the HA that allow the detection of an interruption in the end-to-end tunnel. Tunnels that use IP-in-IP encapsulation do not use keepalive messages. If a tunnel that is using IP-in-IP encapsulation loses its connection to the HA, the mobile router will not be aware of the disruption until it tries to register with the HA again. This can take up to one half of the mobile router’s registration lifetime. GRE keepalive messages allow the status of the end-to-end tunnel to be checked at a configurable interval. If the mobile router detects an interruption in the connection to the HA, it will tear down the existing tunnel and attempt to reregister using the best interface. Typically this is the same interface on which the connection was previously established. If the registration attempt is unsuccessful, the mobile router will then try to register on the next best interface if one exists.

Benefits of GRE for Cisco Mobile Networks

The GRE for Cisco Mobile Networks feature introduces the ability for a mobile router to use GRE tunneling in addition to the default encapsulation method of IP-in-IP. GRE is a widely supported tunneling protocol, and some platforms support GRE tunnels in hardware. Hardware support of GRE tunneling offloads software operations, such as Cisco Express Forwarding (CEF) switching, from the CPU and increases the performance of the router. In addition, GRE supports multiprotocol tunneling and provides explicit protection against recursive encapsulation. Finally, the ability to configure keepalive messages with GRE allows the status of the end-to-end tunnel to be checked at a configurable interval, and reregistration can be attempted as soon as an interruption is detected.

How to Configure GRE for Cisco Mobile Networks

This section contains the following tasks:

- Configuring GRE on the Mobile Router, page 4 (required)
- Configuring GRE Keepalive Messages, page 6 (optional)

Configuring GRE on the Mobile Router

GRE encapsulation can be configured per interface or globally. Configuring GRE encapsulation on an interface allows only that interface to attempt to register with GRE encapsulation enabled. Configuring GRE encapsulation globally allows all roaming interfaces to attempt to register with GRE encapsulation enabled, unless the interface is configured for IP-in-IP encapsulation. The interface-level configuration overrides the global configuration.

Perform one of the following tasks to configure GRE on the mobile router:

- Configuring GRE Globally on the Mobile Router, page 4
- Configuring GRE per Interface on the Mobile Router, page 5

Configuring GRE Globally on the Mobile Router

Perform this task to configure GRE globally on the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile router**
4. **tunnel mode gre**
5. **end**
6. **show ip mobile router registration**
7. **show ip mobile router**

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	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 4	**tunnel mode gre** **Example:** `Router(mobile-router)# tunnel mode gre`	Sets the global encapsulation mode on all roaming interfaces of a mobile router to GRE. **Note** Configuring an encapsulation protocol on an interface overrides the globally configured encapsulation protocol on that interface only. If there is no interface-level configuration, the interface inherits the global configuration.
Step 5	**end** **Example:** `Router(mobile-router)#` **`end`**	Ends the current configuration session and returns to privileged EXEC mode.
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuring GRE per Interface on the Mobile Router

Perform this task to configure GRE on an interface of the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service tunnel mode** {**gre** | **ipip**}
5. **end**
6. **show ip mobile router registration**
7. **show ip mobile router interface**

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 serial 2`	Configures an interface type and enters interface configuration mode.
Step 4	**ip mobile router-service tunnel mode** {**gre** | **ipip**} **Example:** `Router(config-if)# ip mobile router-service tunnel mode gre`	Sets the encapsulation mode for a mobile router interface. • **gre**—Specifies that the mobile router will attempt to register with GRE encapsulation on the interface. • **ipip**—Specifies that IP-in-IP encapsulation will be used on the interface. **Note** Configuring an encapsulation protocol on an interface overrides the globally configured encapsulation protocol on that interface only. If there is no interface-level configuration, the interface inherits the global configuration.
Step 5	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 7	**show ip mobile router interface** **Example:** `Router# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming.

Configuring GRE Keepalive Messages

Perform this task on the mobile router to enable GRE keepalive messages. No configuration is required on the HA to respond to GRE keepalive messages from the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *interface-number*
4. **exit**
5. **keepalive** [**period** [**retries**]]
6. **ip mobile router**
7. **template tunnel** *interface-number*

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 tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 121`	Enters interface configuration mode for the specified interface.
Step 4	**keepalive** [**period** [**retries**]] **Example:** `Router(config-if)# keepalive 5 3`	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 6	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 7	**template tunnel** *interface-number* **Example:** `Router(mobile-router)# template tunnel 121`	Applies a tunnel template to tunnels brought up at the mobile router.

Configuration Examples for GRE for Cisco Mobile Networks

The following sections contain configuration examples for the GRE for Cisco Mobile Networks feature:

- Configuring GRE for Cisco Mobile Networks Globally: Example, page 8
- Configuring GRE for Cisco Mobile Networks on an Interface: Example, page 8
- Verifying GRE for Cisco Mobile Networks: Examples, page 8

Configuring GRE for Cisco Mobile Networks Globally: Example

The following example globally configures GRE encapsulation on a mobile router and enables GRE keepalive messages:

```
router mobile
!
ip mobile secure home-agent 10.40.40.1 spi 101 key hex 12345678123456781234567812345678
     algorithm md5 mode prefix-suffix
ip mobile router
 address 10.80.80.1 255.255.255.0
 home-agent 10.40.40.1
 mobile-network Ethernet1/3
 mobile-network FastEthernet0/0
 template Tunnel 121
 tunnel mode gre
!
interface tunnel 121
 keepalive 5 3
```

Configuring GRE for Cisco Mobile Networks on an Interface: Example

The following example configures GRE encapsulation on an interface of a mobile router and enables GRE keepalive messages:

```
interface FastEthernet0/0
 ip address 10.52.52.2 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service tunnel mode gre
!
interface tunnel 121
 keepalive 5 3
!
ip mobile router
 template tunnel 121
```

Verifying GRE for Cisco Mobile Networks: Examples

The following example shows display output from the **show ip mobile router registration** command when GRE encapsulation is configured on the mobile router. The Flags field shows that GRE encapsulation is enabled by displaying a capital "G." If GRE encapsulation were not enabled, a lowercase "g" would be displayed.

```
Router# show ip mobile router registration

Mobile Router Registrations:
```

```
Foreign agent 10.52.52.1:
    Registration accepted 01/11/00 07:01:24, On FastEthernet0/0
    Care-of addr 10.52.52.1, HA addr 10.40.40.1, Home addr 10.80.80.1
    Lifetime requested 10:00:00 (36000), Granted 01:00:00 (3600)
    Remaining 00:59:47
    Flags sbdmG-t-, Identification B68B7673.81565B8
    Register next time 00:59:27
    Extensions:
        Mobile Network 172.16.153.0/24
        Mobile Network 172.16.143.0/24
        MN-HA Authentication SPI 101
```

The following example shows display output from the **show ip mobile router** command when GRE encapsulation is globally configured on the mobile router. When GRE encapsulation is enabled, the line "Request GRE tunnel" is displayed in the output and the tunnel mode is shown as "GRE/IP".

```
Router# show ip mobile router

Mobile Router
    Enabled 01/11/00 06:59:19
    Last redundancy state transition NEVER

Configuration:
    Home Address 10.80.80.1 Mask 255.255.255.0
    Home Agent 10.40.40.1 Priority 100 (best) (current)
    Registration lifetime 65534 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 20, Retry 10, Interval 1
    Request GRE tunnel
    Mobile Networks:Ethernet1/3 (172.16.143.0/255.255.255.0)
                     FastEthernet0/0 (172.16.153.0/255.255.255.0)

Monitor:
    Status -Registered-
    Active foreign agent 10.52.52.1, Care-of 10.52.52.1
    On interface FastEthernet0/0
    Tunnel0 mode GRE/IP
```

The following example shows display output from the **show ip mobile router interface** command when GRE encapsulation is configured on an interface of the mobile router. When GRE encapsulation is enabled on the interface, the line "Request GRE tunnel" is displayed in the output.

```
Router# show ip mobile router interface

FastEthernet0/0:
    Priority 110, Bandwidth 100000, Address 10.52.52.2
    Periodic solicitation disabled, Interval 600 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Current 2000, Remaining 0 msec, Count 2
    Hold down 0 sec
    Routing disallowed
    Collocated CoA disabled
    Request GRE tunnel
```

Additional References

The following sections provide references related to the GRE for Mobile Networks 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
Mobile IP commands and configuration tasks related to mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 12.2(13)T
Additional information about GRE keepalives	*Generic Routing Encapsulation (GRE) Tunnel Keepalive* feature document, Release 12.2(8)T
Information on configuring quality of service (QoS) with GRE	Quality of Service Options on GRE Tunnel Interfaces

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*.

- **ip mobile router-service tunnel mode**
- **show ip mobile router**
- **show ip mobile router interface**
- **tunnel mode gre**

Glossary

agent advertisement—An advertisement message constructed by an attachment of a special extension to an ICMP Router Discovery Protocol (IRDP) to advertise mobility services to potential users.

agent discovery—The method by which a mobile node or mobile router determines whether it is currently connected to its home network or a foreign network and detects whether it has moved and the way it has moved. It is the mechanism by which mobile nodes or mobile routers query and discover mobility agents. Agent discovery is an extension to ICMP Router Discovery Protocol (IRDP) (RFC 1256), which includes a mechanism to advertise mobility services to potential users.

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.

FA—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.

GRE—generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

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

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. Registration may happen directly from the mobile node to the home agent or through a foreign agent.

tunnel—The path followed by a packet while it is encapsulated from the home agent to the mobile node. The model is that, while the packet is encapsulated, it is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

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

Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

First Published: June 22, 2006
Last Updated: November 17, 2006

The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature extends support for Network Address Translation (NAT) traversal to the mobile router when the mobile router is in private addressing space behind a NAT-enabled device and needs to register directly to the public home agent using a private collocated care-of address (CCoA).

NAT traversal is based on the RFC 3519 specification and defines how Mobile IP should operate to traverse networks that deploy NAT within their network. NAT traversal allows Mobile IP to interoperate with networks that have NAT enabled by providing an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added that establish User Datagram Protocol (UDP) tunneling.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router" section on page 10.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

The mobile router should have the ability to obtain a CCoA on the visited network.

Restrictions for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

- If the network does not allow communication between a UDP port chosen by a mobile node and UDP port 434 on the home agent, the Mobile IP registration and the data tunneling will not work.
- Only UDP/IP encapsulation is supported.

Information About Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Before you configure the Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Access Router feature, you should understand the following concepts:

This document uses the terms “mobile node” and “mobile router.” Most of the conceptual information in this document applies to both a mobile node and a mobile router. The term “mobile router” also applies to the Cisco 3200 Mobile Access Router. Refer to the “Glossary” section for definitions of these terms.

NAT Traversal Support Overview

Network Address Translation (NAT) is a mechanism that conserves address space by reducing the need for globally unique IP addresses. NAT is designed to allow networks with private addressing schemes to exchange traffic with public networks. However, NAT can conflict with the delivery of Mobile-IP-encapsulated traffic for a mobile node (or mobile router) that resides behind a NAT-enabled router.

In Mobile IP, usually IP-in-IP tunneling or generic routing encapsulation (GRE) tunneling allows traffic to be sent between the home agent or mobile nodes either directly or through a foreign agent. These tunneling mechanisms do not generally contain enough information to permit unique translation from the public address to the particular care-of address (CoA) of a mobile node or foreign agent that resides behind the NAT-enabled router. Specifically, there are no TCP/UDP port numbers to permit unique translation of the private CoA into the public address. Thus, the traffic from the mobile node cannot be routed even after a successful registration and will always be dropped at the NAT gateway.

NAT traversal solves this problem by using UDP tunneling as an encapsulation mechanism for tunneling Mobile IP data traffic, for both forward and reverse tunneling, between the home agent and foreign agent or between the home agent and mobile node. UDP tunneling is established by the use of new message extensions in the initial Mobile IP registration request and reply exchange that request UDP tunneling. Registration requests and replies do not use UDP tunneling.

UDP-tunneled packets that have been sent by a mobile node use the same ports as the registration request message. 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 a home agent use the same ports, but in reverse.

When the registration request packet traverses a NAT-enabled router, the home agent detects the traversal by comparing the source IP address of the packet with the CoA inside the request. If the two addresses differ, the home agent detects that a NAT gateway exists in the middle. If the home agent is configured to accept NAT traversal, it accepts the registration request and enables the use of UDP tunneling, and the data traffic passes through the NAT gateway. Thereafter, any traffic from the home agent to the mobile node is sent through the UDP tunnel. If there is a foreign agent, the foreign agent must also be configured for NAT traversal in order for UDP tunneling to work. See the "Mobile IP Support for NAT Traversal on the Mobile Router Feature Design" section for information about the scenario in which the mobile router chooses to register with the home agent using a private CCoA.

By setting the force bit in the UDP tunneling request, the mobile node or mobile router can request that Mobile IP UDP tunneling be established regardless of the NAT detection outcome by the home agent. This capability can be useful in networks that have firewalls and other filtering devices that allow TCP and UDP traffic but do not support NAT translation. The final outcome of whether the mobile node or mobile router will receive UDP tunneling is determined by whether the home agent is configured to accept such requests.

NAT devices are designed to drop the translation state after a period of traffic inactivity over the tunnel. NAT traversal support has implemented a keepalive mechanism that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel. The keepalive messages are sent to ensure that NAT keeps the state information associated with the session and that the tunnel stays open.

The keepalive timer interval is configurable on the home agent, the mobile router, and the foreign agent but is controlled by the home agent keepalive interval value sent in the registration reply. When the home agent sends a keepalive value in the registration reply, the mobile node, mobile router, or foreign agent must use that value as its keepalive timer interval.

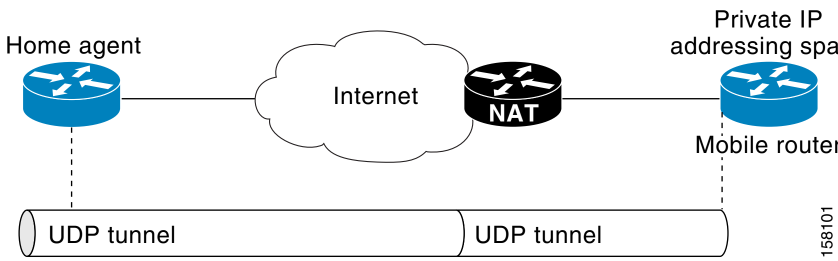
The keepalive timer interval configured on the foreign agent or mobile router is used only if the home agent returns a keepalive interval of zero in the registration reply.

Mobile IP Support for NAT Traversal on the Mobile Router Feature Design

The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature was designed for the scenario where the mobile router is behind a NAT-enabled router and needs to register directly to the home agent using a private CCoA address.

If configured for NAT traversal, the mobile router will request UDP tunneling in its registration request. If the home agent is configured for NAT traversal, the home agent will send a registration reply stating that it will accept UDP tunneling. Upon receiving this reply, the mobile router will create a UDP tunnel with the agreed-upon encapsulation type. The mobile router will also enable the periodic keepalive message between the mobile router and the home agent. If there is a keepalive failure or if there is no keepalive response from the home agent for three or more successive registration requests, the mobile router will terminate the UDP tunnel and will restart the registration process. Figure 1 shows the UDP tunnel that was set up between the home agent and the mobile router.

Figure 1 Topology Showing the UDP Tunnel Between the Home Agent and the Mobile Router



How to Configure the Mobile Router for RFC 3519 NAT Traversal Support

This section contains the following tasks:

- Configuring the Mobile Router for NAT Traversal Support, page 4 (required)
- Configuring the Home Agent for NAT Traversal Support, page 5 (required)
- Verifying Mobile Router NAT Traversal Support, page 6 (optional)

Configuring the Mobile Router for NAT Traversal Support

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service collocated registration nat traversal** [**keepalive** *seconds*] [**force**]
5. **end**

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 FastEthernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip mobile router-service collocated registration nat traversal [keepalive** *seconds***] [force]** **Example:** `Router(config-if)# ip mobile router-service collocated registration nat traversal keepalive 45 force`	Enables NAT traversal support for the mobile router. The keywords and arguments are as follows: • **keepalive** *seconds*—(Optional) Configures the keepalive interval, in seconds, that the mobile router will use when the home agent does not offer a specific value and just returns zero. The range is from is 0 to 65535. The default is 110. **Note** Setting the *keepalive-time* argument to zero disables the keepalive timer. The mobile router does not use the keepalive interval unless the home agent sends back a zero in the registration reply. • **force—**(Optional) Allows the mobile router to force the home agent to allocate a NAT UDP tunnel without performing detection presence of NAT along the HA-MR path. **Note** If you configure the mobile router to force the home agent to allocate a UDP tunnel but do not configure the home agent to force UDP tunneling, the home agent will reject the forced UDP tunneling request. The decision of whether to force UDP tunneling is controlled by the home agent.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring the Home Agent for NAT Traversal Support

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile home-agent nat traversal [keepalive** *seconds***] [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** ***seconds*****] [forced {accept | reject}]** **Example:** `Router(config)# ip mobile home-agent nat traversal keepalive 45 forced accept`	Enables NAT traversal support for the home agent. The keywords and argument are as follows: • **keepalive** *seconds*—(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. • **forced**—(Optional) Enables the home agent to accept or reject forced UDP tunneling from the mobile node regardless of the NAT-detection outcome. – **accept**—Accepts UDP tunneling. – **reject**—Rejects UDP tunneling. This is the default behavior.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying Mobile Router NAT Traversal Support

Perform this task to verify mobile router NAT traversal support.

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]
3. **show ip mobile globals**

4. **show ip mobile tunnel** [*interface*]
5. **show ip mobile router interface**
6. **show ip mobile router registration**
7. **show ip mobile router**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**] **Example:** `Router# show ip mobile binding`	Displays the mobility binding on the home agent.
Step 3	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	Displays global information for mobile agents.
Step 4	**show ip mobile tunnel** [*interface*] **Example:** `Router# show ip mobile tunnel`	Displays active tunnels.
Step 5	**show ip mobile router interface** **Example:** `Router# show ip mobile router interface`	Displays information about the interfaces configured for roaming.
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays pending and/or accepted registrations of the mobile router.
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuration Examples for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

This section provides the following configuration example:

- Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router: Example, page 8

Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router: Example

The following example shows how to configure NAT traversal between the home agent and the mobile router.

Home Agent Configuration

```
interface Loopback1
 ip address 198.168.2.1. 255.255.255.255
!
router mobile
!
! The following command sets the UDP keepalive interval to 60 seconds 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
```

Mobile Router Configuration

```
interface Loopback1
! Description MR's home address.
ip address 10.99.100.2 255.255.255.255
!
interface FastEthernet0/0
 description Wi-Fi Link
 ip address 10.5.3.32 255.255.255.0
! The following command sets the UDP keepalive interval to 60 seconds and enables the
! mobile router to request UDP tunneling.
 ip mobile router-service collocated registration nat traversal keepalive 60 force
 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
```

Additional References

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

Related Documents

Related Topic	Document Title
Mobile IP information and configuration tasks	*Cisco IOS IP Mobility Configuration Guide*, Release 12.4
Mobile IP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Mobility Command Reference*, Release 12.4T
Information about NAT Traversal Support for Mobile IP	*Mobile IP Support for RFC 3519 NAT Traversal*, Cisco IOS Release 12.3(8)T feature module
Cisco 3200 Series Mobile Access Router documentation	*Cisco 3200 Series Mobile Access Router Software Configuration Guide*

Standards

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

MIBs

MIB	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

RFC	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
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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 router-service collocated registration nat traversal**

Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/fn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Feature Name	Releases	Feature Information
Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router	12.4(6)XE 12.4(11)T	The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature extends support for NAT traversal to the mobile router when the mobile router is in private addressing space behind a NAT-enabled device and needs to register directly to the public home agent using a private CCoA. In Cisco IOS Release 12.4(11)T, the feature name changed from Mobile IP Support for RFC 3519 NAT Traversal on the Cisco 3200 Mobile Router to Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router.

Glossary

agent advertisement—An advertisement message constructed by an attachment of a special extension to an ICMP Router Discovery Protocol (IRDP).

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.

CDPD—cellular digital packet data. Open standard for two-way wireless data communication over high-frequency cellular telephone channels. Allows data transmissions between a remote cellular link and a NAP. Operates at 19.2 kbps.

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.

GPRS—general packet radio service. A service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for Global System for Mobile Communications (GSM) networks.

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*.

home network—The network, possibly virtual, whose network prefix equals the network prefix of the home address of a mobile node.

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

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.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. Registration may happen directly from the mobile node to the home agent or through a foreign agent.

tunnel—The path followed by a packet while it is encapsulated from the home agent to the mobile node. The model is that, while it is encapsulated, a packet is routed to a knowledgeable de-encapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Mobile IP— Policy and Application-Based Routing for MR Multipath

First Published: June 19, 2006
Last Updated: March 11, 2009

Mobile IP has increasingly become important because the public safety and public transportation are likely to adopt multiple wireless technologies to support their mission-critical applications and new services. Before the introduction of the Mobile IP—Mobile Router Multipath Support feature, the Cisco implementation of Mobile IP supported only one tunnel between the mobile router (MR) and the home agent (HA). You must use only one tunnel and one wireless technology at a given time. This feature provides support for multiple paths, and thus multiple wireless technologies, between the mobile router and the home agent and allows user traffic to be load-balanced over all available interfaces.

Finding Feature Information

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Mobile IP - Policy and Application-Based Routing for MR Multipath" section on page 22.

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

Contents

Prerequisites for Mobile IP— Policy and Application-Based Routing for MR Multipath

- Both the HA and the MR must be configured for multipath support.
- The security association between the MR and the HA must be established in order for registrations to succeed.

Restrictions for Mobile IP— Policy and Application-Based Routing for MR Multipath

Policy-based application routing has the following restrictions:

- When you change the mobile-map configuration or ACL template configuration while a registration is active, the existing dynamic mobile maps and ACLs get deleted and new ones are generated. This occurs when the user exits the "mobile-map" configuration submode.
- Priority-based multipath registration is enabled by default and is the only mode.
- Label-based application routing is disabled by default on both the MR and the HA. It can be enabled separately on the MR and HA.
- Application routing does not require multipath to be configured. It works in single-path mode too. Only one "match" clause is permited in each mobile-map entry.
- ACL templates on the HA can be configured with a destination address. If such an ACL is used to generate a dynamic ACL, that dynamic ACL ignores the configured destination address and uses the MR's mobile-network(s) instead.

Information About Mobile IP— Policy and Application-Based Routing for MR Multipath

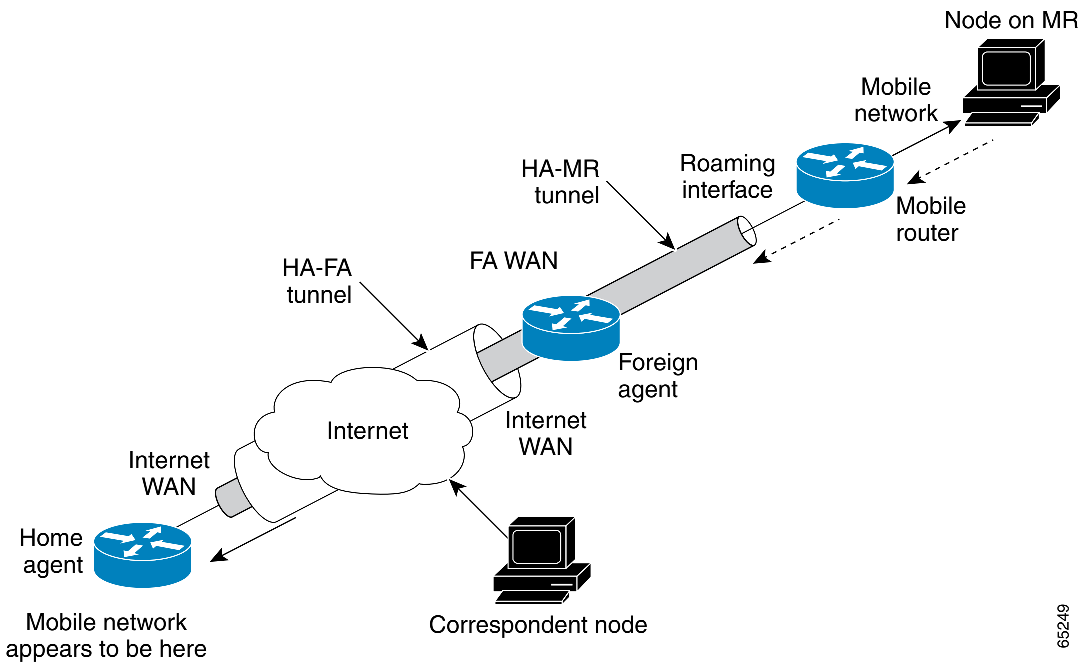
Before you configure the Mobile Router Multipath Support feature and policy-based application routing, you should understand the following concepts:

- Mobile Router Multipath Support Feature Design, page 3
- Mobile Router Multipath Load-Balancing Behavior, page 4
- Benefits of Mobile Router Multipath Support, page 4

Mobile Router Multipath Support Feature Design

The Mobile Router Multipath Support feature extends the MR functionality to multiple interfaces. Before the introduction of this feature, the MR received agent advertisements or a collocated care-of address (CCoA) on multiple roaming interfaces. However, it would register through only one interface and set up the tunnel and routes based on that registration. During the routing or tunneling phase, packets arrived at the HA. The HA performed two encapsulations of the packets and tunneled them to the foreign agent or CCoA. The foreign agent or CCoA performed one de-encapsulation and sent the packets to the MR, which performed another de-encapsulation. The MR then sent the original packets to the IP devices on the mobile networks. See Figure 1 for an illustration of routing within a mobile network using a single tunnel.

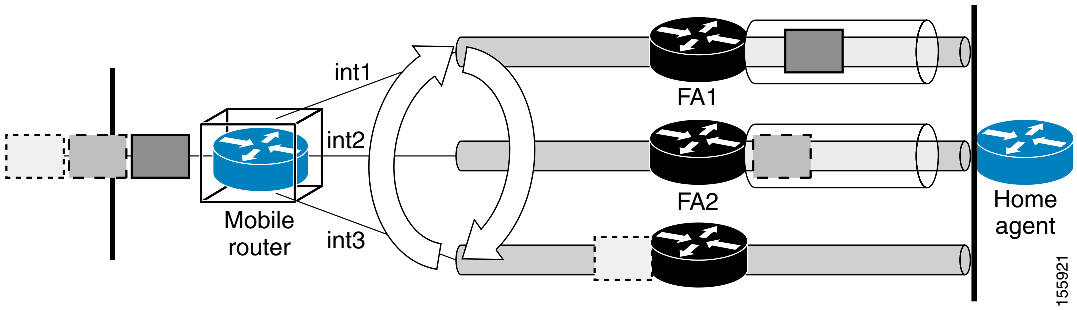
Figure 1 Routing Within the Mobile Network Using a Single Tunnel



With the introduction of the Mobile Router Multipath support feature, the MR can register to the HA through all of its available roaming interfaces. Each registration is independent of the other registrations that occur on the other roaming interfaces. Once registered through more than one roaming interface, the MR has multiple routes to the HA. If a reverse tunnel is configured, the MR will have multiple paths—each tunnel going out its respective interface. Because the MR is registering independently on each of its roaming interfaces, it can use a foreign agent to register on one interface or a CCoA to register with another interface.

See Figure 2 for an illustration of the mobile router registering through multiple interfaces.

Figure 2 Mobile Router Registering Through Multiple Interfaces to the Home Agent



Upon successful registration, the HA maintains multiple care-of addresses, mobility bindings, tunnels, and routes to the same MR. Multiple bindings are not the same as simultaneous bindings. With multiple bindings, the traffic is not replicated on all tunnels but rather load-balanced across them, which means that the packets are sent through only one path.

Mobile Router Multipath Load-Balancing Behavior

When there are multiple paths between the MR and the HA, the traffic from the mobile networks that goes toward the HA is generally load-balanced. Per-destination load balancing is the default behavior. But you can also make use of an advanced behavior, policy-based application routing. Policy-based application routing allows you to identify a particular type of traffic from the mobile networks and then select the tunnel for routing this traffic.

Policy-based application routing allows you to control the roaming interface that is used by an application to route its traffic to the other end of a Mobile IP tunnel. This provides flexibility to control how the applications are routed over different mobile wireless networks based on a defined policy. The applications are policy-routed based on the roaming interface type. See the "Routing Based on Policies and Selecting Roaming Interfaces" section on page 7 for more information on policy-based application routing.

Benefits of Mobile Router Multipath Support

Because multiple access technologies can be deployed in mobile networks, the Mobile Router Multipath support feature offers the ability to leverage all available links when Mobile IP is used. This multiple path support offers good investment protection for existing legacy wireless connections or any newly purchased or deployed wireless technologies.

How to Configure Mobile Router Multipath Support

The Mobile Router Multipath support feature is enabled by default on the MR but is disabled by default on the HA. For this feature to work, both the HA and the MR must be configured for multipath support. Because this feature is enabled by default on the MR, the MR will try for multiple registrations. However, if the MR determines that the HA is not configured for multipath support by receiving registration replies without multiple path support, the MR will switch to single-path mode. This feature is disabled by default on the HA so that during deployments, upgrading the software does not surprise the deployment engineer with multiple registrations.

After configuring the MR, you can configure the policy-based application routing and the MR roaming interfaces. You then need to enable the roaming interfaces and define the traffic policies. This allows you to identify a particular type of traffic from the mobile networks and then select the tunnel for routing the traffic. This provides flexibility to control how the applications are routed over different mobile wireless networks based on a policy.

This section contains the following tasks:

- Configuring the Mobile Router for Multipath Support, page 5
- Routing Based on Policies and Selecting Roaming Interfaces, page 7
- Configuring the Home Agent for Multipath Support, page 13
- Clearing the Mobility Binding on the Home Agent, page 15
- Verifying Mobile Router Multipath Support, page 16

Configuring the Mobile Router for Multipath Support

This task shows how to configure the mobile router for multipath support.

Prerequisites

The security association between the MR and the HA should be established in order for registrations to succeed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **exit**
6. **router mobile**
7. **exit**
8. **ip mobile router**
9. **address** *address mask*
10. **home-agent** *ip-address*
11. **mobile-network** *interface-type interface number*

12. **multi-path** [**metric** {**bandwidth** | **hopcount**}]
13. **end**

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 loopback0`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Sets a primary IP address of the interface. • This is the home address of the mobile router.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 6	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router and enters router configuration mode.
Step 7	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 8	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 9	**address** *address mask* **Example:** `Router(mobile-router)# address 209.165.200.225 255.255.255.224`	Sets the home IP address and network mask of the mobile router.

	Command or Action	Purpose
Step 10	**home-agent** *ip-address* **Example:** `Router(mobile-router)# home-agent 192.0.2.19`	Specifies the home agent that the mobile router uses during registration.
Step 11	**mobile-network** *interface-type interface number* **Example:** `Router(mobile-router)# mobile-network Ethernet3/0`	Specifies the mobile router interface that is connected to the mobile network.
Step 12	**multi-path** [**metric** {**bandwidth** | **hopcount**}] **Example:** `Router(mobile-router)# multi-path`	Enables the mobile router to request multiple path support. • Bandwidth is the default metric.
Step 13	**end** **Example:** `Router(mobile-router)# end`	Returns to privileged EXEC mode.

Routing Based on Policies and Selecting Roaming Interfaces

This section contains the following topics:

Prerequisites

Policy-based application routing occurs only when an ingress interface is configured for a mobile policy.

Setting Priority Levels and MR Registration

You can configure policy-based application routing and the MR roaming interfaces. You should set the priority levels when you enable the roaming interface. The MR registers on multiple roaming interfaces based on the roaming interface configuration. The MR registers only through the highest priority interface. If there is more than one interface with the same highest priority, then both interfaces are used by the MR during registration. If all highest priority interfaces are unavailable, then the MR switches to the next available highest priority interface. The interfaces have link-type labels configured on them. See "Registering the MR Based on the Roaming Priority: Example" section on page 19 for an example.

A label is used to describe a link-type associated with a roaming interface. The label indicates the path such as, link type, actual bandwidth, or stability. You need to manually configure the label on a roaming interface using the **ip mobile router-service link-type** command.

Example:

```
interface ethernet 1/0
 ip mobile router-service roam
 ip mobile router-service link-type 802.11g
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service roam priority** *priority level*
5. **end**

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 FastEthernet0/2`	Configures an interface and enters interface configuration mode.
Step 4	**ip mobile router-service roam priority** *priority-level* **Example:** `Router(config-if)# ip mobile router-service roam priority 101`	Enables the roaming interface and sets the priority level. The roaming interface priority defaults to 100 if priority is not specified while configuring the **ip mobile router-service roam** command.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Enabling the Roaming Interfaces

You can enable the roaming interfaces after setting the roaming priority level. The MR registers on multiple roaming interfaces based on the roaming-interface configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service roam priority** *priority-level*
5. **ip mobile router-service link-type** *label*
6. **end**

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 FastEthernet0/2`	Configures an interface and enters interface configuration mode.
Step 4	**`ip mobile router-service roam priority`** *`priority-level`* **Example:** `Router(config-if)# ip mobile router-service roam priority 101`	Enables the roaming interface and sets the priority level. The roaming interface priority defaults to 100 if priority is not specified while configuring the **ip mobile router-service roam** command.
Step 5	**`ip mobile router-service link-type`** *`label`* **Example:** `Router(config-if)# ip mobile router-service link-type 802.11g`	Enables a link-type roaming interface.
Step 6	**`end`** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.

Defining the Traffic Policies

You can define the traffic policies by identifying the application traffic and selecting the path for routing based on policies. This section contains the following tasks:

- Identifying the Application Traffic, page 10
- Selecting the Routing Path, page 11

Identifying the Application Traffic

You can use one or more extended named ACLs on both the MR and the HA to identify the application traffic. MR and HA named ACLs are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list name*
4. **permit udp any any eq** *port*
5. **end**

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 access-list extended** *access-list name* **Example:** `Router(config)# ip access-list extended WEB`	Configures an extended named ACL.
Step 4	**permit udp any any eq** *port* **Example:** `Router(config-ext-nacl)# permit udp any any eq 8080`	Identifies the application traffic to be policy routed. These are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route-maps.
Step 5	**end** **Example:** `Router(config-ext-nacl)# end`	Returns to privileged EXEC mode.

Selecting the Routing Path

You can use one or more mobile-map mobile policy templates on the MR and HA to select the routing path.

Multiple mobile policies can be configured on either the MR or the HA. On the MR, a separate dynamic route map is generated for each configured mobile policy. More than one MR ingress interface (mobile network interface) has a mobile policy and each interface has a different policy. On the HA there is only one dynamic route map generated, but it is applied on up to three ingress interfaces. If more than one mobile policy is configured on the HA, only one route map is dynamically generated and applied to the ingress interface(s).

You need to apply the mobile map to access interfaces. The mobile map is associated with a mobile network interface on the MR in the “mobile-network” configuration. The mobile-map configuration on the HA can specify up to three "ingress" interfaces.

When traffic from a mobile network is received by the MR, the traffic is compared against one of the ACLs. If there is a match, the MR finds the corresponding mobile-map entry that specifies the roaming interface on which to send the traffic. Similarly, on the HA when traffic for a mobile network is received on one of the specified ingress interfaces, it is matched against one of the ACLs and then against the corresponding mobile-map entry, which in turn decides the tunnel to send the traffic to.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service roam priority** *priority-level*
5. **ip mobile router-service link-type** *label*
6. **exit**
7. **ip access-list extended** *access-list name*
8. **permit udp any any eq** *port*
9. **exit**
10. **ip mobile mobile-map** *map name*
11. **match access-list** *acl*
12. **set link-type** *label*
13. **set interface** *interface-type number*
14. **ip mobile router**
15. **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	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/2`	Configures an interface and enters interface configuration mode.
Step 4	**ip mobile router-service roam priority** *priority level* **Example:** `Router(config-if)# ip mobile router-service roam priority 101`	Enables the roaming interface and sets the priority level. • The roaming interface priority defaults to 100 if priority is not specified while configuring the **ip mobile router-service roam** command.
Step 5	**ip mobile router-service link-type** *label* **Example:** `Router(config-if)# ip mobile router-service link-type 802.11g`	Enables a link-type roaming interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**ip access-list extended** *access-list-name* **Example:** `Router(config)# ip access-list extended WEB`	Configures an extended named ACL and enters interface configuration mode.
Step 8	**permit udp any any eq** *port* **Example:** `Router(config-ext-nacl)# permit udp any any eq 8080`	Identifies the application traffic to be policy routed. The extended named ACLs on both the MR and HA are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route maps.
Step 9	**exit** **Example:** `Router(config-ext-nacl)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 10	**ip mobile mobile-map** *map name* **Example:** `Router(config)# ip mobile mobile-map MPATH_1 10`	Configures mobile policy templates on the MR and HA.
Step 11	**match access-list** *acl* **Example:** `Router(config)# match access-list WEB`	Specifies an ACL name.
Step 12	**set link-type** *label* **Example:** `Router(config)# set link-type 802.11a GPRS`	Specifies up to three link-type labels.
Step 13	**set interface** *interface-type number* **Example:** `Router(config)# set interface Ethernet1/0`	Specifies the interface for dropping traffic.
Step 14	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Applies the mobile map to ingress interfaces in the MR and to up to three ingress interfaces in the HA.
Step 15	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Configuring the Home Agent for Multipath Support

This task shows how to configure the HA for multipath support.

You can configure and unconfigure multipath support globally on the HA. Unconfiguring multiple paths takes the mobile router back to the existing single-path mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router mobile**
4. **exit**
5. **ip mobile home-agent multi-path** [**metric** {**bandwidth** | **hopcount**}]
6. **ip mobile virtual-network** *net mask* [**address** *address*]
7. **ip mobile host** *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*}
8. **ip mobile mobile-networks** *lower* [*upper*]
9. **register**

10. **multi-path** [**metric** {**bandwidth** | **hopcount**}]
11. **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	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router and enters router configuration mode.
Step 4	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 5	**ip mobile home-agent multi-path** [**metric** {**bandwidth** | **hopcount**}] **Example:** `Router(config)# ip mobile home-agent multi-path`	Enables the home agent to process registration requests with multiple path support for all mobile routers. • Bandwidth is the default metric.
Step 6	**ip mobile virtual-network** *net mask* [**address** *address*] **Example:** `Router(config)# ip mobile virtual-network 209.165.200.225 255.255.255.224`	Defines a virtual network. Specifies that the home network is a virtual network, which means that the mobile router is not physically attached to the home agent. Adds the network to the home agent's forwarding table so that routing protocols can redistribute the subnet.
Step 7	**ip mobile host** *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*} **Example:** `Router(config)# ip mobile host 209.165.200.219 255.255.255.224 virtual-network 209.165.200.225 255.255.255.224`	Configures the mobile router as a mobile host. The IP address is in the home network. • The **interface** *name* option configures a physical connection from the home agent to the mobile router.
Step 8	**ip mobile mobile-networks** *lower* [*upper*] **Example:** `Router(config)# ip mobile mobile-networks 209.165.200.219 209.165.200.225`	Configures mobile networks for the mobile host and enters mobile networks configuration mode. The *upper* range can be used only with dynamically registered networks and allows you to configure multiple mobile routers at once. • The range must be within the range configured in the **ip mobile host** command.

	Command or Action	Purpose
Step 9	**register** **Example:** `Router(mobile-networks)# register`	Dynamically registers the mobile networks with the home agent.
Step 10	**multi-path** [**metric** {**bandwidth** | **hopcount**}] **Example:** `Router(mobile-networks)# multi-path`	Configures the global default setting and enables the home agent to process requests with multiple path support for a specific mobile router. Bandwidth is the default metric.
Step 11	**exit** **Example:** `Router(mobile-networks)# no multi-path`	Returns to privileged EXEC mode.

What to Do Next

After you configure the HA you can define the traffic policies. This enables you to identify a particular traffic from the mobile networks and then select the tunnel for routing the traffic. This provides flexibility to control how the applications are routed over different mobile wireless networks based on a policy. See the ""Defining the Traffic Policies" section on page 10" for more information on how to define the traffic policies.

Clearing the Mobility Binding on the Home Agent

Perform this task to manually clear the mobility binding that is associated with the MR IP address and its care-of address.

Restrictions

Use this **clear** command with care, because it will disrupt any sessions that are being used by the MR. After you use this command, the mobile router will need to re-register to continue roaming.

SUMMARY STEPS

1. **enable**
2. **clear ip mobile binding** *mr-ip-address* [**coa** *care-of-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`clear ip mobile binding`** *`mr-ip-address`* `[`**`coa`** *`care-of-address`*`]` **Example:** `Router# clear ip mobile binding 192.0.2.72`	Removes mobility bindings. • You can remove a specific care-of address or all care-of addresses associated with a mobile router.

Verifying Mobile Router Multipath Support

Perform this task to verify MR multipath support.

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]
3. **show ip mobile global**
4. **show ip mobile mobile-networks**
5. **show ip mobile tunnel** [*interface*]
6. **show ip route**
7. **show ip mobile router**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**] **Example:** `Router# show ip mobile binding`	Displays the mobility binding on the home agent.
Step 3	**show ip mobile global** **Example:** `Router# show ip mobile global`	Displays global information for mobile agents.
Step 4	**show ip mobile mobile-networks** **Example:** `Router# show ip mobile mobile-networks`	Displays a list of mobile networks that are associated with the mobile router.
Step 5	**show ip mobile tunnel** [*interface*] **Example:** `Router# show ip mobile tunnel`	Displays active tunnels.
Step 6	**show ip route** **Example:** `Router# show ip route`	Displays the current state of the routing table.
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuration Examples for Mobile Router Multipath Support

This section provides the following configuration examples:

Multipath Support on the Mobile Router: Example

The following example shows how to configure multipath support on the mobile router:

```
interface Loopback0
! MR home address
 ip address 209.165.200.225 255.255.255.224
interface Tunnel101
 keep 5 3
interface Ethernet1/0
! MR roaming interface
 ip address 209.165.200.239 255.255.255.224
 ip mobile router-service roam
interface Ethernet2/0
! MR roaming interface
 ip address 209.165.200.246 255.255.255.224
 ip mobile router-service roam
interface Ethernet3/0
 ip address 209.165.200.247 255.255.255.224
router mobile
ip mobile router
 address 209.165.200.251 255.255.255.224
 home-agent 192.0.2.12
 mobile-network Ethernet3/0
 tunnel mode gre
 multi-path
 template Tunnel101
ip mobile secure home-agent 192.0.2.16 spi 101 key hex 12345678901234567890123456789012
```

Multipath Support on the Home Agent: Example

The following example shows how to configure multipath support on the home agent:

```
interface Ethernet 0/0
 ip address 209.165.200.251 255.255.255.224
!
router mobile
 exit
 ip mobile home-agent multi-path
 ip mobile virtual-network 209.165.200.252 255.255.255.224
 ip mobile host 192.0.2.10 192.0.2.15 virtual-network 209.165.200.254 255.255.255.224
 ip mobile secure host 192.0.2.20 192.0.2.25 spi 101 key hex
 12345678901234567890123456789012
ip mobile mobile-networks 192.0.2.40 192.0.2.44
 register
ip mobile mobile-networks 192.0.2.57
```

```
 register
 no multi-path
```

Registering the MR Based on the Roaming Priority: Example

The following example shows how roaming priority levels are selected during MR registration:

Consider the following four interfaces:

```
interface Fastethernet 1/0
  ip mobile router-service roam priority 200
  ip mobile router-service link-type 802.11g
interface Fastethernet 1/1
  ip mobile router-service roam priority 200
  ip mobile router-service link-type 802.11g
interface Fastethernet 2/0
  ip mobile router-service roam priority 100
  ip mobile router-service link-type 802.11g
interface Fastethernet 2/1
  ip mobile router-service roam priority 100
  ip mobile router-service link-type 802.11g
```

Fast Ethernet interfaces 1/0 and 1/1 have priority 200. Fast Ethernet interfaces 2/0 and 2/1 have priority 100. When you try enabling these four interfaces, the MR registers on both the Fast Ethernet interfaces 1/0 and 1/1 because they have the highest roaming priority. But when the interfaces Fastethernet 1/0 and 1/1 are not available, the MR registers on Fastethernet 2/0 and 2/1, the next available highest priority group.

Using mobile-map Mobile Policy Templates: Example

The following example shows to use the mobile-map mobile policy templates on the MR and the HA to select the routing path.

```
ip mobile mobile-map MPATH_1 10
 match access-list WEB
 set link-type 802.11g UMTS
 set interface null0
```

Generating Dynamic Route Maps in an HA: Example

The following example shows how the dynamic route maps are generated in an HA:

```
Router# show route-map dynamic
route-map MIP-10/24/06-04:18:15.243-1-MP-HA, permit, sequence 0, identifier 53856096
  Match clauses:
    ip address (access-lists): VOICE-to-192.0.2.0/24
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1

Router# show ip access-lists dynamic
Extended IP access list VOICE-to-192.0.2.0/24
    10 permit icmp any 209.165.200.225 255.255.255.224 tos max-reliability
```

Additional References

The following sections provide references related to the Mobile IP— Policy and Application-Based Routing for MR Multipath Support feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Mobility Command Reference*

Standards

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

MIBs

MIB	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

RFC	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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

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, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **clear ip mobile binding**
- **debug ip mobile dyn-pbr**
- **ip mobile home-agent multi-path**
- **ip mobile router-service link-type**
- **ip mobile router-service roam**
- **multi-path (mobile networks)**
- **multi-path (mobile router)**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile mobile-networks**
- **show ip mobile router interface**
- **show ip mobile router registration**
- **show ip mobile tunnel**

Feature Information for Mobile IP - Policy and Application-Based Routing for MR Multipath

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/fn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Mobile IP— Policy and Application-Based Routing for MR Multipath

Feature Name	Releases	Feature Information
Mobile IP—Mobile Router Multipath Support	12.4(9)T	This Mobile IP—Mobile Router Multipath Support feature provides support for multiple paths, and thus multiple wireless technologies, between the mobile router and the home agent and allows user traffic to be load-balanced over all available interfaces.
Mobile IP— Policy and Application-Based Routing for MR Multipath	12.4(24)T	This feature provides support for mobile router multipath registration based on roaming interface priority; application routing based on link or path type; and multiple registrations based on roaming interface priority. The following commands were introduced: **ip mobile router-service link-type**, **ip mobile router-service roam**. The following commands were modified: **show ip mobile binding, show ip mobile router interface, show ip mobile router registration, show ip mobile tunnel**

Glossary

agent advertisement—An advertisement message constructed by an attachment of a special extension to an ICMP Router Discovery Protocol (IRDP).

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.

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

home network—The network, possibly virtual, whose network prefix equals the network prefix of the home address of a mobile node.

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

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.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

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

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. Registration may happen directly from the mobile node to the home agent or through a foreign agent.

roaming interface—An interface used by the mobile router to detect foreign agents and home agents while roaming. Registration and traffic occur on the interface.

tunnel—The path followed by a packet while it is encapsulated from the home agent to the mobile node. The model is that, while it is encapsulated, a packet is routed to a knowledgeable decapsulating agent, which de-encapsulates the datagram and then correctly delivers it to its ultimate destination.

Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing

The Mobile Router DHCP Support for Dynamic Collocated Care-of Address (DCCoA) and Foreign Agent (FA) Processing feature adds support for mobile router roaming on Ethernet interfaces that acquire an IP address dynamically via the Dynamic Host Configuration Protocol (DHCP). The interface can register using this acquired IP address as a DCCoA or register using a CoA acquired from a foreign agent. This behavior is true for all platforms that support Mobile IP beginning with Cisco IOS Release 12.3(14)T.

This feature adds support for FA processing of advertisements and registrations on DHCP roaming interfaces.

A Simple Network Management Protocol (SNMP) signaling capability is also added to support this feature on the Cisco 3200 Series Mobile Access Router with a Wireless Mobile Interface Card (WMIC). The WMIC uses SNMP trap messages to signal the mobile router that the Layer 2 wireless local-area network (WLAN) is either up or down.

Feature History for the Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing Feature

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Mobile Router DHCP Support for DCCoA and FA Processing

There are no prerequisites for DHCP support. However, if a Cisco 3200 Series Mobile Access Router is using a WMIC, the WMIC should be configured for SNMP traps. The 802.11 Layer 2 transitions (associations and disassociations) that take place on the WMIC are signaled to the mobile router via SNMP. Specifically, the Interface MIB linkUp and linkDown traps are sent to the mobile router Ethernet or VLAN interface.

See the *Configuration Guide for the Cisco 3200 Series Mobile Access Router* for more information on how to configure SNMP traps on the Cisco 3200 Series router.

Restrictions for Mobile Router DHCP Support for DCCoA and FA Processing

The Mobile IP process will only process SNMP signals from a WMIC. The SNMP signaling functionality for DCCoA is supported on the Cisco 3200 Series Mobile Access Router.

The linkDown and linkUp trap events will not trigger mobile router redundancy.

Information About Mobile Router DHCP Support for DCCoA and FA Processing

Before you configure this feature, you should understand the following concepts:

Care-of Addresses

If a mobile router determines that it is connected to a foreign network, it acquires a CoA. This CoA is the exit point of the tunnel from the home agent toward the mobile router. The CoA is included in the mobile router's registration request and is used by the home agent to forward packets to the mobile router in its current location. There are two types of CoAs:

- CoA acquired from a foreign agent
- Collocated care-of address (CCoA)

A foreign agent CoA is an IP address on a foreign agent that is advertised on the foreign network being visited by a mobile router. A foreign agent CoA can be shared by other mobile routers.

A CCoA is an IP address assigned to the interface of the mobile router itself. A CCoA represents the current position of the mobile router on the foreign network and can be used by only one mobile router at a time. A CCoA can be static or dynamic. A static CCoA is a fixed IP address configured on an interface. A dynamic CCoA is an IP address dynamically acquired via DHCP on an Ethernet interface or Point-to-Point Protocol (PPP)/IP Control Protocol (IPCP) on a point-to-point serial interface.

An interface enabled for both foreign agent CoA and CCoA registration will always register a foreign agent CoA instead of a CCoA if a foreign agent CoA is available.

Mobile Router DHCP Support

This feature introduces DCCoA and foreign agent CoA support when IP addresses are obtained via DHCP on a roaming interface. Prior to the introduction of this feature, the mobile router could only support foreign agent CoA registration, static CCoA registration, and DCCoA registration through PPP/IPCP.

For both static and dynamic CCoA, the interface can be configured to exclusively use the CCoA for registration or to use a foreign agent CoA if one is available. An interface enabled for both foreign agent CoA and CCoA registration will always register a foreign agent CoA instead of a CCoA if a foreign agent CoA is available.

In the foreign agent case, when an interface first comes up, it will attempt to discover foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile router will register using the advertised CoA. The interface will continue to register using a CoA as long as a foreign agent is heard. When foreign agents are not heard, CCoA processing is enabled and the interface registers its CCoA. The CCoA is the interface's statically configured or dynamically acquired primary IP address. If a foreign agent is heard again, the interface will again register using the foreign agent CoA.

In previous releases of CCoA support, the CCoA registration would begin only after a number of solicits were sent or no advertisements were heard. For faster roaming, this delay is now eliminated. Now the interface registers a foreign agent CoA if an agent advertisement is heard or it registers a CCoA if an address is acquired, depending on which event occurs first. In the case where the interface registers a CCoA first, a subsequent receipt of an agent advertisement will then cause the interface to register with the foreign agent.

To support CCoA on Ethernet interfaces, a default gateway address is required. This gateway address is used as the default gateway for CCoA registration and as a default route after the interface is registered. For static CCoA on an Ethernet interface, a default gateway address must be provided through the roaming interface CCoA configuration. See the Cisco IOS Release 12.2(15)T *Mobile Networks Static Collocated Care-of Address* feature documentation for configuration details.

When an interface is configured for DCCoA via DHCP, a configured gateway address is not required and the option to configure a gateway address is not offered through the command line interface (CLI). For DHCP interfaces, DCCoA registration uses the DHCP default router address and, once the interface is registered, the address is also used for the mobile router default route and gateway.

Mobile Router Support for SNMP Traps

On a Cisco 3200 Series Mobile Access Router with a WMIC, SNMP traps allow the roaming interface to determine when the connected WLAN link status changes. Without this signaling, a CCoA-registered interface would not be aware of link status changes. The mobile router must be configured to receive SNMP linkUp and linkDown traps from the WMIC and can then make roaming decisions based on the type of trap received.

Mobile Router Processing of linkUp Traps

When a linkUp trap is received on a DHCP roaming interface, the mobile router interface will either renew the current IP address or acquire a new IP address as quickly as possible. If the interface already has a DHCP-acquired IP address, the mobile router will attempt to renew it first. If renewal fails, the interface will attempt to acquire a new IP address.

If a DHCP interface is without an IP address, DHCP address acquisition begins. Address "discovery" attempts are repeated at increasing intervals (up to 60 seconds) and continue until an address is acquired. During address discovery, the interface is "IP-enabled" and IP packets can be processed. This means that foreign agent CoA advertisements can be heard and Mobile IP registration can take place, even though the interface does not have an IP address.

The new **ip dhcp client mobile renew** command allows you to configure the number of renewal attempts and the interval between attempts for renewing the current IP address that was acquired through DHCP. The configured values override any default values.

For roaming purposes, the roaming interface treats a linkUp trap event the same as if the roaming interface just came up. For example, solicits are sent, if foreign agent CoA-enabled, and the mobile router determines if this interface, compared to other roaming interfaces, should register. Dynamic address acquisition can trigger a DCCoA registration.

If the interface is already registered when the linkUp trap arrives and nothing else has changed that affects the registration decision, the mobile router will retain the existing registration.

Mobile Router Processing of linkDown Traps

Receipt of a valid linkDown trap starts a new, configurable reassociation hold-down timer. The purpose of this timer is to delay the mobile router's response to the trap, which is typically an attempt to register on the next best interface, for a period of time long enough for the WMIC to reassociate with another bridge or access point (AP). The mobile router remains registered during this hold-down period, foreign agent data is retained, and the mobile router interface keeps any DHCP-acquired IP address. The hold-down timer should be set to the maximum time it should take the WMIC to re-establish wireless connectivity while roaming between adjacent bridges or APs.

If a linkUp trap arrives before the hold-down timer expires, the mobile router remains registered and foreign agent data is retained. Solicits are sent to find foreign agents and the DHCP IP address renewal and discovery process begins. If the WMIC has roamed to an AP on the same subnet, address renewal should succeed.

If the hold-down timer expires or the hold-down delay was set to 0, mobile router processing proceeds as if the interface just went down. Any foreign agents heard on this interface are deleted from the foreign agent list and, if registered on the interface, the mobile router deletes the current registration and tries to register by using the next best roaming interface. Solicits are sent to find foreign agents and the DHCP IP address renewal and discovery process begins.

Benefits of Mobile Router DHCP Support for DCCoA and FA Processing

This feature allows a mobile router to roam to foreign networks where foreign agents may or may not be deployed and where IP addresses are obtained dynamically via DHCP. The SNMP trap capability permits the Cisco 3200 Series Mobile Access Router with a WMIC to respond to changes in the WLAN link status.

How to Configure Mobile Router DHCP Support for DCCoA

This section contains the following procedures:

- Enabling DHCP Support for DCCoA Processing on a Mobile Router Interface, page 5 (required)
- Configuring SNMP on the Mobile Router, page 7 (optional)
- Verifying the Dynamic CCoA Configuration, page 8 (optional)

Enabling DHCP Support for DCCoA Processing on a Mobile Router Interface

Perform this task to enable dynamic CCoA processing on a mobile router interface through DHCP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address dhcp**
5. **ip dhcp client mobile renew count** *number* **interval** *msec*
6. **ip mobile router-service roam**
7. **ip mobile router-service collocated** [**ccoa-only**]
8. **ip mobile router-service hold-down reassociate** *msec*

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 FastEthernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	**`ip address dhcp`** **Example:** `Router(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP. • DHCP address acquisition time can be reduced by turning off the pings normally sent out by the DHCP server to verify that the IP address is not in use. If using a Cisco IOS router as a DHCP server, use the **ip dhcp ping packets** *number* command and set the *number* argument to 0 (zero).
Step 5	**`ip dhcp client mobile renew count`** *`number`* **`interval`** *`msec`* **Example:** `Router(config-if)# ip dhcp client mobile renew count 4 interval 25`	(Optional) Configures the number of renewal attempts and the interval between attempts for renewing the current IP address acquired by DHCP. • By default the interface will attempt to renew its address twice and wait 50 milliseconds between attempts. You only need to use this command if you want to adjust the number of attempts or the interval between attempts.
Step 6	**`ip mobile router-service roam`** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.

	Command or Action	Purpose
Step 7	**ip mobile router-service collocated** [**ccoa-only**] **Example:** `Router(config-if)# ip mobile router-service collocated`	Enables CCoA processing on a mobile router interface. • The interface will first solicit foreign agent advertisements and register with a foreign agent CoA if an advertisement is heard. If no advertisements are received, CCoA registration is attempted. • The **ccoa-only** keyword enables the interface to use CCoA processing only.
Step 8	**ip mobile router-service hold-down reassociate** *msec* **Example:** `Router(config-if)# ip mobile router-service hold-down reassociate 2000`	(Optional) Specifies the delay, after receiving a linkDown trap, that the mobile router waits for a linkUp trap. • The default is 1000 msec. The range is from 0 to 5000 seconds. • This reassociate hold-down period is the interval of time (in milliseconds) that the mobile router will wait, after receiving an SNMP linkDown trap, for a linkUp trap from the WMIC indicating that the wireless link is available for use.

Configuring SNMP on the Mobile Router

If a Cisco 3200 Series Mobile Access Router is using a WMIC, the router must be configured for SNMP. The WMIC uses SNMP trap messages to signal the mobile router that the WLAN is either up or down. See the *Configuration Guide for the Cisco 3200 Series Mobile Access Router* for additional information on how to configure SNMP traps.

Perform this task to configure SNMP on the mobile router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server engineID remote** *remote-ip-address remote-engineID-string*
4. **snmp-server user** *username group-name* **remote** *remote-ip-address* **v3**

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	**`snmp-server engineID remote`** *`remote-ip-address remote-engineID-string`* **Example:** `Router(config)# snmp-server engineID remote 172.21.58.1 800000090300000F23AD8F30`	Specifies the SNMP engine ID of a remote SNMP device.
Step 4	**`snmp-server user`** *`username group-name`* **`remote`** *`remote-ip-address`* **`v3`** **Example:** `Router(config)# snmp-server user labusr labgrp remote 172.21.58.1 v3`	Configures a new user to an SNMP group.

Verifying the Dynamic CCoA Configuration

To verify the dynamic CCoA configuration, perform the following steps.

SUMMARY STEPS

1. **show ip mobile router interface**
2. **show ip mobile router agent**
3. **show ip mobile router registration**
4. **show ip mobile router**
5. **show ip mobile binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip mobile router interface** **Example:** `Mobilerouter# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming. • If the interface is configured for CCoA, the CCoA (IP address) is displayed even if the interface is down. • If the interface is configured for DCCoA via DHCP, the Layer 2 linkDown hold-down value and the most recently processed link state trap will be displayed.
Step 2	**show ip mobile router agent** **Example:** `Mobilerouter# show ip mobile router agent`	Displays information about the agents for the mobile router. • If the interface configured for CCoA is up, an entry is shown.
Step 3	**show ip mobile router registration** **Example:** `Mobilerouter# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 4	**show ip mobile router** **Example:** `Mobilerouter# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
Step 5	**show ip mobile binding** **Example:** `Homeagent# show ip mobile router`	Displays the mobility binding table. • If a CCoA is registered with the home agent, (D) direct-to-mobile node is displayed in the Routing Options field.

Configuration Examples for Mobile Router DHCP Support for DCCoA

This section provides the following configuration example:

• Mobile Router DCCoA Acquired Through DHCP: Example, page 9

Mobile Router DCCoA Acquired Through DHCP: Example

The following example shows a mobile router configured to obtain a CCoA dynamically through DHCP:

Mobile Router

```
! This is the roaming interface using DCCoA
interface FastEthernet0
 ip address dhcp
 ip dhcp client mobile renew count 3 interval 20
 ip mobile router-service roam
 ip mobile router-service collocated
 ip mobile router-service hold-down reassociate 2000
```

```
!
! Receive v1 or v2 traps
snmp-server community public RO
snmp-server enable traps tty
!

! Receive v3 traps
snmp-server engineID remote 85.85.85.3 1234
snmp-server user labusr labgrp remote 85.85.85.2 v3 auth md5 <SNMP user password on WGB>
snmp-server group labgrp v3 auth
```

Additional References

The following sections provide references related to the Mobile Router DHCP Support for DCCoA and FA Processing feature.

Related Documents

Related Topic	Document Title
Cisco 3200 Series Mobile Access Router documentation	*Configuration Guide for the Cisco 3200 Series Mobile Access Router*
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 12.3T
Mobile IP commands and configuration tasks related to mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 12.2(13)T
Static CCoA documentation	*Mobile Networks Static Collocated Care-of Address* feature document, Release 12.2(15)T
Dynamic CCoA documentation	*Mobile Networks Dynamic Collocated Care-of Address* feature document, Release 12.3(4)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 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*.

- **ip dhcp client mobile renew**
- **ip mobile router-service**
- **show ip mobile router agent**
- **show ip mobile router interface**

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.

collocated care-of address—The termination point of a tunnel toward a mobile node or mobile router. A CCoA is a local address that the mobile node or mobile router associated with one of its own network interfaces.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses and other configuration parameters dynamically so that addresses can be reused when hosts no longer need them.

foreign agent—A router on the visited network of a foreign network that provides routing services to the mobile node or mobile router 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.

IPCP—IP Control Protocol. The protocol used to establish and configure IP over PPP.

PPP—Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is most commonly used for dial-up Internet access. Its features include address notification, authentication via CHAP or PAP, support for multiple protocols, and link monitoring.

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

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

Mobile Ad Hoc Networks for Router-to-Radio Communications

First Published: May 17, 2007
Last Updated: October 2, 2009

Mobile Ad Hoc Networks (MANET) for router-to-radio communications address the challenges faced when merging IP routing and mobile radio communications in ad hoc networking applications. the Cisco solution for MANETs provides capabilities that enable

- Optimal route selection based on Layer 2 feedback from the radio network
- Faster convergence when nodes join and leave the network
- Efficient integration of point-to-point, directional radio topologies with multi hop routing
- Flow-controlled communications between each radio and its partner router

Through the router-to-radio link, the radio can inform the router immediately when a node joins or leaves, and this enables the router to recognize topology changes more quickly than if it had to rely on timers. Without this link-status notification from the radio, the router would likely time out while waiting for traffic. The link-status notification from the radio enables the router to respond faster to network topology changes. Metric information regarding the quality of a link is passed between the router and radio, enabling the router to more intelligently decide on which link to use.

With the link-status signaling provided by the router-to-radio link, applications such voice and video work better because outages caused by topology changes are reduced or eliminated. Sessions are more stable and remain active longer.

Finding Feature Information

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information About the Mobile Ad Hoc Networks for Router-to-Radio Communications" section on page 75.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for Mobile Ad Hoc Networks for Router-to-Radio Communications

The features described in this document require one of the following router platforms:

- Cisco 2800 Series (2801, 2811, 2821, or 2851)
- Cisco 3250 and Cisco 3270
- Cisco 3800 Series (3825 or 3845)

To use the PPPoE and virtual multipoint interface (VMI) features described in this document, a radio device that implements the PPPoE functionality enhancements described in the draft RFC 2516 is required. Users can optionally implement draft-bberry-pppoe-credit-06.txt for *PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics*, but this draft must be implemented if you plan to use VMI features.

Restrictions for Mobile Ad Hoc Networks for Router-to-Radio Communications

VMI on Routed Ports

VMIs can be configured only on routed ports. VMIs are not supported on VLAN or switched ports.

Quality of Service

Of the Quality of Service (QoS) queueing features available from Cisco, only class-based Weighted Fair Queueing (WFQ) is supported on VMIs. The VMI can identify Differentiated Services Code Point (DSCP) values, and perform network-based application recognition (NBAR), but no policing or policy mapping occurs on those matches.

Information About Mobile Ad Hoc Networks for Router-to-Radio Communications

This section describes VMI PPPoE. The following sections are included:

Benefits of Router-to-Radio Links Using Virtual Multipoint Interfaces with PPPoE in Cisco IOS Software

As the global leader in mission-critical networking and IP communications, Cisco is uniquely positioned to deliver reliable and efficient converged voice, video, and data solutions to organizations around the world. Benefits of this technology include the following:

- Optimal route selection is based on Layer 2 feedback from the radio network.
- Efficient integration of point-to-point, directional radio topologies with multi hop routing.
- Convergence is faster when nodes join and leave the network because routers are able to respond faster to network topology changes.
- Flow-controlled communications between the radio and its partner router enables applications such voice and video to work better because outages caused by moving links are reduced or eliminated. Sessions are more stable and remain active longer.

MANETs for Router-to-Radio Communications

Mobile Ad Hoc Networks (MANETs) enable users deployed in areas with no fixed communications infrastructure to access critical voice, video, and data services. Soldiers in the field can employ unified communications, multimedia applications, and real-time information dissemination to improve situational awareness and respond quickly to changing battlefield conditions. Disaster managers can use video conferences, database access, and collaborative tools to coordinate multi-agency responses within an Incident Command System (ICS) framework. For event planners and trade show managers, MANETs represent a cost-effective way to accommodate mobile end users on a short term basis. MANETs set the stage for more timely information sharing and faster, more effective decision-making.

In MANET environments, highly mobile nodes communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network router, with the two devices interconnected over an Ethernet. Since these nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET becomes a challenge because the state of a node can change well before the event is detected by the normal timing mechanisms of the routing protocol.

Radio link quality in a MANET can vary dramatically because it can be affected by a variety of factors such as noise, fading, interference, and power fluctuation. As a result, avoiding congestion and determining optimal routing paths also pose significant challenges for the router network. Finally, directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multi-hop, multipoint router environments, as it increases the size of each router’s topology database and reduces routing efficiency.

Effective networking in a MANET environment therefore requires mechanisms by which

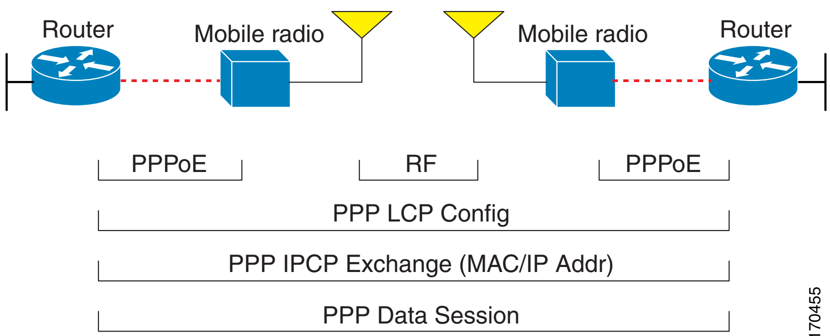
- routers and radios can interoperate efficiently, and without impacting operation of the radio network
- radio point-to-point and router point-to-multipoint paradigms can be rationalized
- radios can report status to routers for each link and each neighbor, and
- routers can use this information to optimize routing decisions.

PPPoE Interfaces for Mobile Radio Communications

The Cisco MANET solution employs PPP-over-Ethernet (PPPoE) sessions to enable intra-nodal communications between a router and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (router-to-router); This is duplicated each time a radio establishes a new radio link. The Virtual Multipoint Interface (VMI) on the router aggregates multiple PPPoE sessions and multiplexes these to look like a single interface to the routing processes. This interface collects the series of PPP/PPPoE connections. Underneath the VMI interface there are virtual access interfaces that are associated with each of the PPP/PPPoE connections.

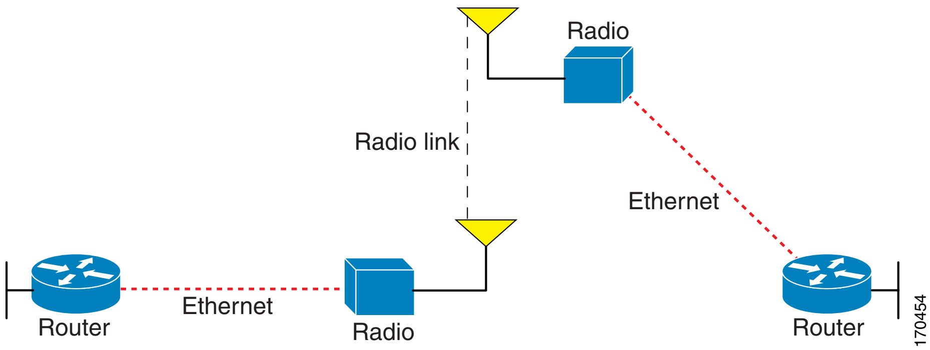
A PPPoE session is established between a router and a radio on behalf of every other router/radio neighbor located in the MANET. These Layer 2 sessions are the means by which radio network status gets reported to the Layer 3 processes in the router. Figure 1 illustrates the PPPoE session exchange between mobile routers and directional radios in a MANET network.

Figure 1 PPPoE Session Exchange Between Mobile Routers and Directional Radios



This capability assumes that a PPPoE-equipped radio connects to a router using Ethernet. The router always considers the Ethernet link to be up. If the radio side of the link goes down, the router will wait until a routing update time-out has occurred to declare the route down and then update the routing table. Figure 2 illustrates a simple router-to-radio link topology.

Figure 2 Router-to-Radio Link



Routing protocols used for VMI PPPoE are EIGRP (IPv4, IPv6) and OSPFv3 (IPv6).

Virtual Multipoint Interface

The VMI interface provides services that map outgoing packets to the appropriate PPPoE sessions based on the next-hop forwarding address for that packet. The VMI interface also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through the VMI interface, VMI replicates the packet and unicasts it to each of its neighbors.

Directional radios are frequently used in applications that require greater bandwidth, increased power-to-transmission range, or reduced probability of detection. These radios operate in a point-to-point mode, and generally have no broadcast capability. On the other hand, the routing processes in Cisco's MANET solution operate most efficiently when viewing the network link as point-to-multipoint, with broadcast capability. For the router, modeling the MANET as a collection of point-to-point nodes would have a dramatic impact on the size of its internal database.

The Virtual Multipoint Interface (VMI) within the router aggregates all of the per-neighbor PPPoE sessions from the Radio Ethernet connection. The VMI maps the sessions to appear to Layer 3 routing protocols and applications as a single point-to-multipoint, multi-access, broadcast-capable network. However, the VMI preserves the integrity of the PPPoE sessions on the radio side, so that each point-to-point connection can have its own Quality of Service (QoS) queue.

The VMI also relays the link quality metric and neighbor up/down signaling from the radio to the routing protocols. Currently, VMI signals are used by EIGRP (for IPv4 and IPv6 neighbors) and OSPFv3 (for IPv6 neighbors).

Link Quality Metrics Reporting for OSPFv3 and EIGRP with VMI Interfaces

The quality of a radio link has a direct impact on the throughput that can be achieved by router-router traffic. The PPPoE protocol has been extended to provide a process by which a router can request, or a radio can report, link quality metric information. Cisco's OSFPv3 and EIGRP implementations have been enhanced so that the route cost to a neighbor is dynamically updated based on metrics reported by the radio, thus allowing the best route to be chosen within a given set of radio links.

The routing protocols receive raw radio link data, and compute a composite quality metric for each link. In computing these metrics, the following factors may be considered:

- Maximum Data Rate – the theoretical maximum data rate of the radio link, in bytes per second

- Current Data Rate – the current data rate achieved on the link, in bytes per second
- Latency – the transmission delay packets encounter, in milliseconds
- Resources – a percentage (0-100) that can represent the remaining amount of a resource (such as battery power)
- Relative Link Quality – a numeric value (0-100) representing relative quality, with 100 being the highest quality

Metrics can be weighted during the configuration process to emphasize or de-emphasize particular characteristics. For example, if throughput is a particular concern, the *current data rate* metric could be weighted so that it is factored more heavily into the composite metric. Similarly, a metric that is of no concern can be omitted from the composite calculation.

Link metrics can change rapidly, often by very small degrees, which could result in a flood of meaningless routing updates. In a worst case scenario, the network would be churning almost continuously as it struggled to react to minor variations in link quality. To alleviate this concern, Cisco provides a tunable dampening mechanism that allows the user to configure threshold values. Any metric change that falls below the threshold is ignored.The quality of a connection to a neighbor varies, based on various characteristics of the interface when OSPF or EIGRP is used as the routing protocol. The routing protocol receives dynamic raw radio link characteristics and computes a composite metric that is used to reduce the effect of frequent routing changes.

A tunable hysteresis mechanism allows users to adjust the threshold to the routing changes that occur when the router receives a signal that a new peer has been discovered, or that an existing peer is unreachable. The tunable metric is weighted and is adjusted dynamically to account for the following characteristics:

- Current and Maximum Bandwidth
- Latency
- Resources
- Hysteresis

Individual weights can be deconfigured and all weights can be cleared so that the cost is set back to the default value for the interface type. Based on the routing changes that occur, cost can be determined by the application of these metrics. The following sections provide more details about OSPF and EIGRP metrics:

- OSPF Cost Calculation for VMI Interfaces, page 6
- EIGRP Cost Metrics for VMI Interfaces, page 8
- VMI Metric to EIGRP Metric Conversion, page 10
- Dynamic Cost Metric for VMI Interfaces, page 11
- EIGRP Metric Dampening for VMI Interfaces, page 11

OSPF Cost Calculation for VMI Interfaces

Because cost components can change rapidly, it might be necessary to dampen the volume of changes to reduce network-wide churn. The recommended values for S2, S3, and S4 are based on network simulations that may reduce the rate of network changes. The recommended value for S1 is zero to eliminate this variable from the route cost calculation.

The overall link cost is computed using the following formula:

$$LinkCost = OC + BW\left(\frac{Throughput\_weight}{100}\right) + Resources\left(\frac{Resources\_weight}{100}\right) + Latency\left(\frac{Latency\_weight}{100}\right) + L2\_factor\left(\frac{L2\_weight}{100}\right)$$

$$OC = \left[\frac{(ospf\_reference\_bw)(1 x 10^{6})}{(MDR)(1024)}\right]$$

Note: The default ospf reference bw is 100

$$BW = \frac{(65535+1)\left(100 - \frac{CDR}{MDR}(100)\right)}{100}$$

$$Resources = \frac{(100 - resources)^{3}(65536)}{100}$$

$$Latency = latency$$

$$L2\_factor = \frac{(100 - RLQ)(65535+1)}{100}$$

231048

Table 1 defines the symbols used in the OSPF cost calculation.

Table 1 OSPF Cost Calculation Definitions

Cost Component	Component Definition
OC	The "default OSPF Cost". Calculated from reference bandwidth using reference_bw / (MDR*1000) where reference_bw=10^8
A through D	Various radio-specific data based formula's which produce result in range 0-64k
A	CDR and MDR related formula (2^16 * (100 - (CDR * 100 / MDR)))/100
B	Resources related formula ((100 - RESOURCES)^3 * 2^16 / 10^6)
C	Latency as reported by the radio (already in the 0-64K range when reported (LATENCY)
D	RLF related formula ((100 - RLF) * 2^16)/100
S1 through S4	Scalar weighting factors input from CLI. These scalars scale DOWN the values as computed by A-D. The value of 0 disables and value of 100 enables full 0-64k range for one component.

While each network might have unique characteristics that require different settings to optimize actual network performance, these are recommended values intended as a starting point for optimizing a OSPFv3 network. Table 2 lists the recommended value settings for OSPF cost metrics.

Table 2 Recommended Value Settings for OSPF Cost Metrics

Setting	Metric Description	Default Value	Recommended Value
S1	ipv6 ospf dynamic weight throughout	100	0
S2	ipv6 ospf dynamic weight resources	100	29
S3	ipv6 ospf dynamic weight latency	100	29
S4	ipv6 ospf dynamic weight L2 factor	100	29

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- FDDI—Default cost is 1.
- X25—Default cost is 5208.
- Asynchronous—Default cost is 10,000.
- ATM— Default cost is 1.

To illustrate these settings, the following example shows how OSPF cost metrics might be defined for a VMI interface:

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

EIGRP Cost Metrics for VMI Interfaces

When EIGRP is used as the routing protocol, metrics allow EIGRP to respond to routing changes. The link-state metric is advertised as the link cost in the router link advertisement.The reply sent to any routing query will always contain the latest metric information. Exceptions which will result in immediate update being sent:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

EIGRP receives dynamic raw radio link characteristics and computes a composite EIGRP metric based on a proprietary formula. To avoid churn in the network as a result of the change in the link characteristics, a tunable dampening mechanism is used.

EIGRP uses the metric weights along with a set of vector metrics to compute the composite metric for local RIB installation and route selections. The EIGRP composite metric is calculated using the formula:

EIGRP Metric = 256*((K1*Bw) + (K2*Bw)/(256-Load) + (K3*Delay)*(K5/(Reliability + K4)))

Table 3 lists the EIGRP vector metrics and their descriptions.

Table 3 EIGRP Vector Metrics

Vector Metric	Description
bandwidth	Minimum bandwidth of the route in kilobits per second. It can be 0 or any positive integer. The bandwidth for the formula is scaled and inverted by the following formula: (**10^7/minimum Bw in kilobits per second**)
delay	Route delay in tens of microseconds.
delay reliability	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.
load	Effective load of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Minimum maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

EIGRP monitors metric weights on an interface to allow for the tuning of EIGRP metric calculations and indicate type of service (TOS). Table 4 lists the K-values and their default.

Table 4 EIGRP K-Value Defaults

Setting	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

Most configurations use the first two metrics –delay and bandwidth, with bandwidth taking precedence. The default formula of 256*(BW +Delay) is the EIGRP metric. The bandwidth for the formula is scaled and inverted by the following formula:

(**10^7/minimum Bw in kilobits per second**)

Note You can change the weights (as with IGRP), but these weights must be the same on all the routers.

For example, look at an IGRP link whose bandwidth to a particular destination is 128k and the delay is 84000 microseconds.

Using the cut-down formula, the EIGRP metric calculation would simplify to 256*(BW + Delay), resulting in the following value:

Metric = 256*(10^7/128 + 84000/10)= 256*86525 = 22150400

To calculate route delay, divide the delay value by 10 to get the true value in tenths of microseconds

When calcluating the delay for MANET and the delay is obtained from a router interface, it is always calculated in tens of microseconds. In most cases, when using MANET, you will not use the interface delay, but rather the delay that is advertised by the radio. The delay you will receive from the radio is in microseconds, so you must adjust the cut-down formula as follows:

Metric = (256*(10^7/128) + (84000*256)/10) = 20000000 + 2150400 = 22150400

VMI Metric to EIGRP Metric Conversion

The quality of connection to a VMI neighbor will vary based on various characteristics computed dynamically based on the feedback from L2 to L3. Table 5 lists the EIGRP metrics and their significance.

Table 5 EIGRP MANET Metrics for VMI Interfaces

Metric	Significance
current data rate	Snapshot value of bytes per second rate on the link
max data rate	Bytes per second maximum rate on link
latency	Average delay on the link, specified in ms
resources	A representation of resources indicating a percentage (0-100), such as, battery power. Harris implementation always reports 100
relative link quality	opaque number (0-100) representing radio's view of link quality 0 represents the worst possible link, 100 represents the best.

These EIGRP vector metric values map to the basic EIGRP interface parameters as indicated in Table 6

Table 6 Mapping of VMI Metric Values to EIGRP Vector Metrics Values

VMI Metric	EIGRP Metric	Mapping
current data rate	Bandwidth	Used directly and is converted to kilobits.
relative link quality resources	Reliability	Calculated according to the following formula: if resources < 30% (255 * ((relative link quality + resources)/2) / 100 else (255 * relative link quality) / 100
max data rate relative link quality	Delay	Calculated according to the following formula: **calc_delay**(maximum_data_rate) * 100 / relative link quality) / USEC_TO_MSEC. The value used for USEC_TO_MSEC is 1000.
load	Load	Calculated according to the following formula: ((255 * load) / 100)

Note If the current data rate = 0; then (current data rate / max data rate) is defined to be 1.

Note calc_delay is a function which checks the value against well-known delay/bandwidth values. If it does not match a well-known value, the formula used is 10,000,000,000 / max_data_rate.

Dynamic Cost Metric for VMI Interfaces

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). The dynamic cost is calculated using the following formula:

L2L3API

Where the metric calculations are

S1 = ipv6 ospf dynamic weight throughput
S2 = ipv6 ospf dynamic weight resources
S3 = ipv6 ospf dynamic weight latency
S4 = ipv6 ospf dynamic weight L2 factor
OC = standard cost of a non-VMI route

Throughput = (current-data-rate)/(maximum-data-rate)

Router-dynamic cost= OC + (S1) + (S2) + (S3) + (S4)

For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the Open Shortest Path First (OSPF) cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored

EIGRP Metric Dampening for VMI Interfaces

Because metric components could be changing rapidly, the frequency of the changes can have an impact on the network. Frequent changes require that prefixes learned though the VMI interface be updated and sent to all adjacencies. This update can result in further updates and, in a worst-case scenario, cause network-wide churn. To prevent such effects, metrics can be dampened, or thresholds set, so that any change that does not exceed the dampening threshold is ignored.

Network changes that cause an immediate update include

- a down interface
- a down route
- any change in a metric which results in the router selecting a new nexthop

Dampening the metric changes can be configured based on change or time intervals.

If the dampening method is change-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, will not be advertised to adjacencies until the computed metric changes from the last advertised value significantly enough to cause an update to be sent.

If this dampening method is interval-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, will not be advertised to adjacencies until the specified interval is met, unless the change results in a new route path selection.

When the timer expires, any routes, which have outstanding changes to report, will be sent out. If a route changes, such that the final metric of the route matches the last updated metric, no update will be sent.

Neighbor Up/Down Signaling for OSFPv3 and EIGRP

MANETs are highly dynamic environments. Nodes may move into, or out of, radio range at a fast pace. Each time a node joins or leaves, of course, the network topology must be logically reconstructed by the routers. Routing protocols normally use timer-driven "hello" messages or neighbor timeouts to track topology changes, but for MANETs reliance on these mechanisms can result in unacceptably slow convergence.

This signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the router each time a link to another neighbor is established or terminated by the creation and termination of PPPoE sessions. In the router, the routing protocols (OSPFv3 or EIGRP) respond immediately to these signals by expediting formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the router will immediately sense the loss and establish a new route to the vehicle through neighbors that are not blocked. This high speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When VMI with PPPoE is used and a partner node has left or a new one has joined, the radio informs the router immediately of the topology change. Upon receiving the signal, the router immediately declares the change and updates the routing tables.

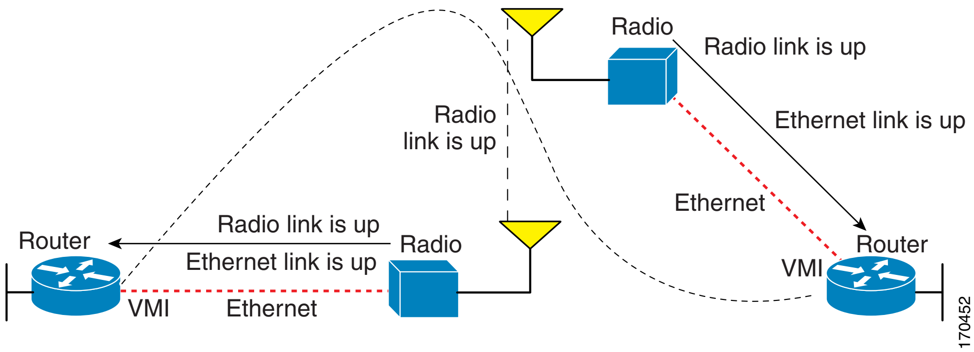
The signaling capability reduces routing delays and prevents applications from timing out; enables network-based applications and information to be delivered reliably and quickly over directional radio links; provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted; and reduces impact on radio equipment by minimizing the need for internal queuing/buffering; also provides consistent Quality of Service for networks with multiple radios.

The messaging allows for flexible rerouting when necessary because of

- Noise on the Radio links
- Fading of the Radio links
- Congestion of the Radio links
- Radio link power fade
- Utilization of the Radio

Figure 3 illustrates the signaling sequence that occurs when radio links go up and down.

Figure 3 Up and Down Signaling Sequence



PPPoE Credit-based Flow Control

Each radio initiates a PPPoE session with its local router as soon as the radio establishes a link to another radio. Once the PPPoE sessions are active for each node, a PPP session is then established end-to-end (router-to-router). This process is duplicated each time a radio establishes a new link.

The carrying capacity of each radio link may vary due to location changes or environmental conditions, and many radio transmission systems have limited buffering capabilities. To minimize the need for packet queuing in the radio, Cisco has implemented extensions to the PPPoE protocol that enable the router to control traffic buffering in congestion situations. Implementing flow-control on these router-to-radio sessions also will allow use of quality of service features such as fair queuing.

The solution utilizes a credit-granting mechanism documented in an IETF informational draft. When the PPPoE session is established, the radio can request a flow-controlled session. If the router acknowledges the request, all subsequent traffic must be flow-controlled. If a flow control session has been requested and cannot be supported by the router, the session is terminated. Typically, both the radio and the router initially grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits have been granted. Credits can be added incrementally over the course of a session.

IPv6 Addresses

You can configure VMI interfaces with IPv6 addresses only, IPv4 addresses only, or both IPv4 and IPv6 addresses.

IPv6 addresses are assigned to individual router interfaces and enable the forwarding of IPv6 traffic globally on the router. By default, IPv6 addresses are not configured and IPv6 routing is disabled.

Note The *ipv6-address* argument in the **ipv6 address** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

The */prefix-length* argument in the **ipv6 address** command is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) A slash mark must precede the decimal value.

Restrictions for IPv6 Addressing

In Cisco IOS Release 12.2(4)T or later releases, Cisco IOS Release 12.0(21)ST, and Cisco IOS Release 12.0(22)S or later releases, the **ipv6 address** or **ipv6 address eui-64** command can be used to configure multiple IPv6 global addresses within the same prefix on an interface. Multiple IPv6 link-local addresses on an interface are not supported.

Prior to Cisco IOS Releases 12.2(4)T, 12.0(21)ST, and 12.0(22)S, the Cisco IOS command-line interface (CLI) displays the following error message when multiple IPv6 addresses within the same prefix on an interface are configured as:

```
Prefix <prefix-number> already assigned to <interface-type>
```

For additional information about IPv6 addressing, refer Implementing IPv6 Addressing in the *Cisco IOS IPv6 Configuration Guide*.

Multicast Support for VMI Interfaces

VMI interfaces operate, by default, in aggregate mode, which means that all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the configured VMI. That is, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI interface will be correctly forwarded to the correct virtual-access interface(s).

If you are running multicast applications that require the virtual-access interfaces to be exposed to applications above Layer 2 directly, you can configure the VMI to operate in bypass mode. Most multicast applications require that the virtual-access interfaces be exposed directly to the routing protocols to insure that that multicast Reverse Path Forwarding (RPF) can operate as expected. When you use the bypass mode, you must define a VMI interface to handle presentation of cross-layer signals such as, neighbor up, neighbor down, and metrics. Applications will be aware of the actual underlying virtual-access interfaces, and will send packets to them directly. Additional information is required on the virtual template configuration. Operating the VMI in bypass mode can cause databases in the applications to be larger than would normally be expected because knowledge of more interfaces is required for normal operation.

After configuring the bypass mode, Cisco recommends that you save the running configuration to NVRAM to override the default mode of operation for VMI to logically aggregate the virtual-access interfaces..

How to Configure Router-to-Radio Links Using VMI PPPoE

This section identifies the tasks that will be used to configure VMI PPPoE. Configuring the VMI PPPoE involves implementing the infrastructure, establishing the IPv4 and IPv6 addressing schemes, and configuring the routing environment. This document contains configuration guidelines only for configuration of PPPoE as it relates to VMIs. For details about configuring PPPoE, refer to the *Cisco IOS Broadband and DSL Configuration Guide*. For details about PPPoE commands, refer to the *Cisco IOS Broadband and DSL Command Reference*.

- Creating a Subscriber Profile for PPPoE Service Selection, page 15 (Required)
- Configuring the PPPoE Profile for PPPoE Service Selection, page 16 (Required)
- Configuring PPPoE on an Ethernet Interface, page 17 (Required)
- Creating and Configuring a Virtual Template for VMI PPPoE, page 18 (Optional)
- Creating and Configuring a VMI Interface for EIGRP IPv4, page 20 (Optional)

- Creating and Configuring a VMI interface for EIGRP IPv6, page 23 (Optional)
- Creating and Configuring a VMI Interface for OSPFv3, page 38(Optional)
- Setting the EIGRP Change-based Dampening Interval for VMI Interfaces using classic-style configuration, page 27 (Optional)
- Setting the EIGRP Change-based Dampening Interval for VMI Interfaces using named-style configuration, page 29 (Optional)
- Setting the EIGRP Interval-based Dampening Interval for VMI Interfaces using classic-style configuration, page 32
- Setting the EIGRP Interval-based Dampening Interval for VMI Interfaces using named-style configuration, page 34
- Enabling Multicast Support on a VMI Interface, page 37 (Optional)
- Creating and Configuring a VMI Interface for OSPFv3, page 38 (Optional)
- Verifying the VMI Configuration, page 42 (Optional)

Creating a Subscriber Profile for PPPoE Service Selection

Perform this task to configure a subscriber profile for PPPoE service selection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **pppoe service manet_radio**
5. **exit**
6. **subscriber authorization enable**
7. **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	**subscriber profile** *profile-name* **Example:** `Router(config)# subscriber profile manet`	Enters Subscriber Profile configuration mode.

	Command or Action	Purpose
Step 4	**pppoe service manet_radio** **Example:** `Router(config-sss-profile)# pppoe service manet_radio`	Adds a PPPoE MANET radio service name to a subscriber profile to enable the use of the VMI interface.
Step 5	**exit** **Example:** `Router(config-sss-profile)# exit`	Returns to the global configuration mode.
Step 6	**subscriber authorization enable** **Example:** `Router(config)# subscriber authorization enable`	Enable Subscriber Service Switch type authorization. This command is required when VPDN is not used.
Step 7	**exit** **Example:** `Router(config)# exit`	Returns to the previleged EXEC mode.

What to Do Next

After you have defined the PPPoE subscriber profile and service, you must apply the definitions to a BBA group.

Configuring the PPPoE Profile for PPPoE Service Selection

Perform this task to associate a subscriber profile with a PPPoE profile. In this configuration, the BBA group name should match the subscriber profile name previously defined in the subscriber profile. In this case, the profile name used as the service name is *manet_radio*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
6. **end**

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	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group1`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that will serve as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Router(config-bba-group)# service profile subscriber-group1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. • The PPPoE configuration that is derived from the subscriber gold_isp_A under the PPPoE profile. Use the **service profile** command with the **refresh** keyword and the *minutes* argument to cause the cached PPPoE configuration to be timed out after a specified number of minutes.
Step 6	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Returns to privileged EXEC mode.

Troubleshooting Tips

Use the **show pppoe session** and **debug pppoe** commands to troubleshoot PPPoE sessions.

Configuring PPPoE on an Ethernet Interface

Perform this task to assign a PPPoE profile to an Ethernet interface.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *interface-name slot/port*
4. **pppoe enable** [**group** *group-name*]
5. **end**

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`** *`interface-name slot/port`* **Example:** `Router(config)# interface ethernet 3/1`	Specifies a Ethernet interface and enters interface configuration mode. Ethernet, Fast Ethernet, and Gigabit Ethernet can be used.
Step 4	**`pppoe enable`** `[`**`group`** *`group-name`*`]` **Example:** `Router(config-if)# pppoe enable group bba1`	Enables PPPoE sessions on an Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface by using the **group** *group-name* option, the interface will use the global PPPoE profile.
Step 5	**`end`** **Example:** `Router(config-if)# end`	(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Creating and Configuring a Virtual Template for VMI PPPoE

To create and configure a virtual template, use the following commands beginning in global configuration mode. Cisco recommends that, when using the virtual template, you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the router to terminate the connection if PPP keepalive packets are missed over a lossy Radio Frequency (RF) link.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. Perform step 5, if you are using IPv4. Perform steps 7 and 8, if you are using IPv6. If you are using both, perform steps 5, 6, and 7.
5. **ip unnumbered** *interface-type interface-number*

6. **ipv6 enable**
7. **ipv6 unnumbered** *interface-type interface-number*
8. **end**

DETAILED STEPS

	Command	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 virtual-template`** *`number`* **Example:** `Router(config)# interface virtual-template` *`1`*	Creates a virtual template, and enters interface configuration mode.
Step 4	Perform step 5, if you are using IPv4. Perform steps 7 and 8, if you are using IPv6. If you are using both, perform steps 5, 6, and 7.	—
Step 5	**`ip unnumbered`** *`interface-type interface-number`* **Example:** `Router(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on an interface without assigning an explicit IP address to the interface.
Step 6	**`ipv6 enable`** **Example:** `Router(config-if)# ipv6 enable`	If you are using IPv6, enter the **ipv6 enable** command to enable IPv6 processing on the interface.
Step 7	**`ipv6 unnumbered`** *`interface-type interface-number`* **Example:** `Router(config-if)# ipv6 unnumbered vmi i`	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.

Step 8	`end`
	
	Example:
	`Router(config-if)# end`
		(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Where To Go Next

Refer to the "Virtual Template Interface Service" chapter in the *Cisco IOS Dial Solutions Configuration Guide* for additional information about configuring the virtual templates.

Examples

You can configure multiple virtual template interfaces for your VMI PPPoE connections. The selection of which virtual template to use is predicated on the service name sent by the radio during PPPoE session establishment. As an example, consider the following configuration:

```
subscriber authorization enable
!
subscriber profile one
pppoe service manet_radio_over_x_band
!
!
subscriber profile two
pppoe service manet_radio_over_c_band
!
!
!
bba-group pppoe one
virtual-template 1
service profile one
!
!
bba-group pppoe two
virtual-template 2
service profile two

!
!
interface Virtual-Template1
.
.
.
!
!
interface Virtual-Template2
.
.
.
```

Using this configuration, any PPPoE request for a session (presentation of a PPPoE Active Discovery Initiate, or PADI packet) with the service name of "manet_radio_over_x_band" would use Virtual-Template1 as the interface to be cloned. Conversely, any PADI presented by the radio with the service name of "manet_radio_over_c_band" would use Virtual-Template2.

Note All service names used for MANET implementations *must* begin with the string "manet_radio".

Creating and Configuring a VMI Interface for EIGRP IPv4

Perform this task to create the VMI interface and associate it with the Ethernet interface on which PPPoE is enabled. When you create a VMI interface, assign the IPv6 or IPv4 address to that VMI interface definition. Do not assign any addresses to the corresponding physical interface.

The radio alerts the router with PADT messages that the layer-2 radio frequency (RF) connection is no longer alive. Cisco recommends that you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the router to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

Note This configuration includes Quality of Service (QoS) fair queueing and service policy applied to the VMI interface. Make certain that any fair queueing left over from any previous configurations is removed before applying the new policy map to the virtual template in the VMI configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **no virtual-template subinterface**
5. **policy-map** *policy-mapname*
6. **class class-default**
7. **fair-queue**
8. **interface virtual-template** *number*
9. **ip unnumbered** *interface-type interface-number*
10. **service-policy output** *policy-mapname*
11. **no keepalive**
12. **interface** *interface-type interface-number*
13. **ip address** *address mask*
14. **no ip redirects**
15. **no ip split-horizon eigrp** *autonomous-system-number*
16. **physical-interface** *interface-type/slot*
17. **exit**
18. **router eigrp** *autonomous-system-number*
19. **network** *network-number ip-mask*
20. **redistribute connected**
21. **end**

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	**ip routing** **Example:** `Router# ip routing`	Enables IP routing on the router.o
Step 4	**no virtual template subinterface** **Example:** `Router# no virtual template subinterface`	Disables the virtual template on the subinterface.
Step 5	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy map fair queue`	Enters policy map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 6	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
Step 7	**fair-queue** **Example:** `Router(config-pmap-c)#` **`fair-queue`**	Enables weighted fair queueing (WFQ) on the interface
Step 8	**interface virtual-template** *number* **Example:** `Router(config-pmap-c)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 9	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on a serial interface without assigning an explicit IP address to the interface
Step 10	**service-policy output** *policy-mapname* **Example:** `Router(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC.
Step 11	**no keepalive** **Example:** `Router(config-if)# no keepalive`	Turns off PPP keepalive messages to the interface.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config-if)#` **`interface vmi`** *`1`*	Specifies the number of the VMI interface.

	Command or Action	Purpose
Step 13	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI interface.
Step 14	**no ip redirect** **Example:** `Router(config)# no ip redirect`	Disables the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
Step 15	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Router(config)# no ip split-horizon eigrp 101`	Disables the split horizon mechanism for the specified session.
Step 16	**physical-interface** *interface-type***/***slot* **Example:** `Router(config-if)#  physical-interface FastEthernet 0/1`	Creates the physical subinterface to be associated with the VMI interfaces on the router.
Step 17	**exit** **Example:** `Router(config-if)#  exit`	Exits the interface configuration mode and returns to the global configuration mode.
Step 18	**router eigrp** *autonomous-system-number* **Example:** `Router(config)# router eigrp 100`	Enables EIGRP routing on the router and identifies the autonomous system number.
Step 19	**network** *network-number ip-mask* **Example:** `Router(config)# network 209.165.200.225 255.255.255.224`	Identifies the EIGRP network.
Step 20	**redistribute connected** **Example:** `Router(config)# redistribute connected`	Redistributes routes from one routing domain into another routing domain.
Step 21	**end** **Example:** `Router(config)# end`	(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Creating and Configuring a VMI interface for EIGRP IPv6

Perform this task to create the VMI interface and associate it with the Ethernet interface on which PPPoE is enabled.

Prerequisites

When you create a VMI interface, assign the IPv6 address to that VMI interface definition.

The radio alerts the router with PADT messages that the layer-2 radio frequency (RF) connection is no longer alive. If you turn off the PPP keepalive messages, it can make CPU usage more efficient and help to avoid the potential for the router to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

Restrictions

Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 cef**
5. **policy-map** *policy-mapname*
6. **class class-default**
7. **fair-queue**
8. **interface virtual-template** *number*
9. **ipv6 enable**
10. **no keepalive**
11. **service-policy output** *policy-mapname*
12. **interface** *interface-type interface-number*
13. **ipv6 address** *address/prefix-length*
14. **ipv6 enable**
15. **ipv6 eigrp** *as-number*
16. **no ipv6 redirects**
17. **no ipv6 split-horizon eigrp** *as-number*
18. **physical-interface** *interface-type/slot*
19. **ipv6 router eigrp**
20. **no shutdown**
21. **redistribute connected**
22. **end**

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 unicast-routing** **Example:** `Router# ipv6 unicast-routing`	Enables IPv6 unicast routing.
Step 4	**ipv6 cef** **Example:** `Router# ipv6 cef`	Enables IPv6 CEF on the router.
Step 5	**policy-map** *policy-map-name* `Router(config-pmap)# policy-map fair-queue`	Enters policy map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 6	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
Step 7	**fair-queue** **Example:** `Router(config-pmap-c)#` **fair-queue**	Enables weighted fair queueing (WFQ) on the interface
Step 8	**interface virtual-template** *number* **Example:** `Router(config-if)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 9	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 routing on the virtual template.
Step 10	**no keepalive** **Example:** `Router(config-if)# no keepalive`	Turns off PPP keepalive messages to the virtual template.

	Command or Action	Purpose
Step 11	**service-policy output** *policy-name* **Example:** `Router(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config)# interface vmi 1`	Creates a VMI interface.
Step 13	**ipv6 address** *address***/***prefix* **Example:** `Router(config-if)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address for the interface.
Step 14	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 routing on the interface.
Step 15	**ipv6 eigrp** *as-number* **Example:** `Router(config-if)# ipv6 eigrp 1`	Enables Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on a specified interface and specifies the Autonomous System (AS) number.
Step 16	**no ipv6 redirect** **Example:** `Router(config-if)# no ipv6 redirect`	Disables the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received
Step 17	**no ipv6 split-horizon eigrp** *as_number* **Example:** `Router(config-if)# no ipv6 split-horizon eigrp 100`	Disables the split horizon for EIGRP IPv6. Associates this command with a specific EIGRP AS.
Step 18	**physical-interface** *interface-type/slot* **Example:** `Router(config-if)# physical-interface FastEthernet 1/0`	Creates the physical subinterface to be associated with the VMI interfaces on the router.
Step 19	**ipv6 router eigrp** *as-number* **Example:** `Router(config-if)# ipv6 router eigrp 100`	Places the router in router configuration mode, creates an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process in IPv6, and allows you to enter additional commands to configure this process.
Step 20	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Restarts a disabled interface or prevents the interface from being shut down.

	Command or Action	Purpose
Step 21	**`redistribute connected`** **Example:** `Router(config-if)# redistribute connected`	Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running. Redistributes IPv6 routes from one routing domain into another routing domain.
Step 22	**`end`** **Example:** `Router(config-if)# end`	(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Change-based Dampening Interval for VMI Interfaces using classic-style configuration

Perform the following tasks to set the change-based dampening interval for VMI interfaces using classic-style configuration:

Prerequisites

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers.

Note You may configure this feature with either an IPv4 or an IPv6 address, or you may use both. If you are using both IPv4 and IPv6, then complete the entire configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **ip address** *address mask*
5. **no ip redirects**
6. **no ip split-horizon eigrp** *autonomous-system-number*
7. **ip dampening-change eigrp** *autonomous-system-number percentage*
8. **ipv6 address** *address*
   or
   ipv6 enable
9. **ipv6 eigrp** *autonomous-system-number*
10. **no ipv6 split-horizon eigrp** *autonomous-system-number*
11. **ipv6 dampening-change eigrp** *autonomous-system-number percentage*
12. **router eigrp** *autonomous-system-number*
13. **network** *address*

14. **ipv6 router eigrp** *autonomous-system-number*
15. **end**

DETAILED STEPS

	Command	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** *interface-type interface-number* **Example:** `Router(config)# interface vmi 1`	Enters interface configuration and creates a VMI interface.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI interface.
Step 5	**no ip redirects** **Example:** `Router(config-if)# no ip redirects`	Prevents the router from sending redirects.
Step 6	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Router(config-if)# no ip split-horizon eigrp 101`	Disables the EIGRP split horizon.
Step 7	**ip dampening-change eigrp** *autonomous-system-number percentage* **Example:** `Router(config-if)# ip dampening-change eigrp 1 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes for IPv4.
Step 8	**ipv6 address** *address* or **ipv6 enable** **Example:** `Router(config)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address.
Step 9	**ipv6 eigrp** *autonomous-system-number* **Example:** `Router(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on the interface.

	Command	Purpose
Step 10	**no ipv6 split-horizon eigrp** *autonomous-system-number* **Example:** `Router(config-if)# no ipv6 split-horizon eigrp 1`	Disables the sending of IPv6 redirects messages on an interface.
Step 11	**ipv6 dampening-change eigrp** *autonomous-system-number percentage* **Example:** `Router(config-if)#ipv6 dampening-change eigrp 1 30`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes for IPv6.
Step 12	**router eigrp** *autonomous-system-number* **Example:** `Router(config-if)# router eigrp 1`	Configures the EIGRP address family process and enters router configuration mode.
Step 13	**network** *address* **Example:** `Router(config-router)# network 209.165.200.225`	Configures the a network address.
Step 14	**ipv6 router eigrp** *autonomous-system-number* **Example:** `Router(config-router)# ipv6 router eigrp 1`	Configures EIGRP routing process in IPV6.
Step 15	**end** **Example:** `Router(config-rtr)#end`	(Optional) Exits the current configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Change-based Dampening Interval for VMI Interfaces using named-style configuration

Perform the following tasks to set the change-based dampening interval for VMI interfaces using named-style configuration:

Prerequisites

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers.

Note You may configure this feature with either an IPv4 or an IPv6 address, or you may use both. If you are using both IPv4 and IPv6, then complete the entire configuration.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **ip address** *address mask*
5. **no ip redirects**
6. **ipv6 address** *address*
   or
   ipv6 enable
7. **router eigrp** *virtual-instance-name*
8. **address-family ipv4 autonomous-system** *autonomous-system-number*
9. **network** *network-address*
10. **af-interface** *interface-name interface-number*
11. **dampening-change** *percentage*
12. **exit**
13. **exit**
14. **address-family ipv6 autonomous-system** *autonomous-system-number*
15. **af-interface** *interface-name interface-number*
16. **dampening-change** *percentage*
17. **end**

DETAILED STEPS

	Command	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** *interface-type interface-number* **Example:** `Router(config)# interface vmi 1`	Enters interface configuration and creates a VMI interface.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI interface.

	Command	Purpose
Step 5	**`no ip redirects`** **Example:** `Router(config-if)# no ip redirects`	Prevents the router from sending redirects.
Step 6	**`ipv6 address`** *`address`* `or` **`ipv6 enable`** **Example:** `Router(config)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address.
Step 7	**`router eigrp`** *`virtual-instance-name`* **Example:** `Router(config-if)# router eigrp name`	Enables EIGRP for IPv6 on the interface.
Step 8	**`address-family ipv4 autonomous-system`** *`autonomous-system-number`* **Example:** `Router(config-router)# address-family ipv4 autonomous-system 1`	Enters address-family configuration mode to configure an EIGRP routing instance.
Step 9	**`network`** *`network-address`* **Example:** `Router(config-router-af)# network 209.165.200.225`	Configures the network address.
Step 10	**`af-interface`** *`interface-name interface-number`* **Example:** `Router(config-router-af)# af-interface vmi 1`	Enters address-family interface configuration mode.
Step 11	**`dampening-change`** *`percentage`* **Example:** `Router(config-router-af-interface)# dampening-change 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family.
Step 12	**`exit`** **Example:** `Router(config-router-af-interface)# exit`	Exits the address-family interface configuration mode.
Step 13	**`exit`** **Example:** `Router(config-router-af)# exit`	Exits the address-family configuration mode and enters the router confiuration mode.
Step 14	**`address-family ipv6`** *`autonomous-system autonomous-system-number`* **Example:** `Router(config-router)# address-family ipv6 autonomous-system 1`	Enters address-family configuration mode to configure an EIGRP routing instance for IPv6.

	Command	Purpose
Step 15	**af-interface** *interface-name interface-number* **Example:** `Router(config-router-af)# af-interface vmi 1`	Enters address-family interface configuration mode.
Step 16	**dampening-change** *percentage* **Example:** `Router(config-router-af-interface)# dampening-change 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface.
Step 17	**end** **Example:** `Router(config-router-af-interface)# end`	(Optional) Exits the current configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Interval-based Dampening Interval for VMI Interfaces using classic-style configuration

Perform this task to set an interval-based dampening interval for VMI interfaces using classic-style configuration.

Prerequisites

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **ip address** *address mask*
5. **no ip redirects**
6. **no ip split-horizon eigrp** *autonomous-system-number*
7. **ip dampening-change eigrp** *autonomous-system-number percentage*
8. **ipv6 address** *address*
   or
   ipv6 enable
9. **ipv6 eigrp** *autonomous-system-number*
10. **no ipv6 split-horizon eigrp** *autonomous-system-number*
11. **ipv6 dampening-interval eigrp** *autonomous-system-number percentage*
12. **router eigrp** *autonomous-system-number*
13. **network** *address*

14. **ipv6 router eigrp** *autonomous-system-number*
15. **end**

DETAILED STEPS

	Command	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** *interface-type interface-number* **Example:** `Router(config)# interface vmi 1`	Enters interface configuration and creates a VMI interface.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI interface.
Step 5	**no ip redirects** **Example:** `Router(config-if)# no ip redirects`	Prevents the router from sending redirects.
Step 6	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Router(config-if)# no ip split-horizon eigrp 101`	Disables the EIGRP split horizon.
Step 7	**ip dampening-interval eigrp** *autonomous-system-number interval* **Example:** `Router(config-if)# ip dampening-change eigrp 1 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 8	**ipv6 address** *address* or **ipv6 enable** **Example:** `Router(config)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address.
Step 9	**ipv6 eigrp** *autonomous-system-number* **Example:** `Router(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on the interface.

	Command	Purpose
Step 10	**no ipv6 split-horizon eigrp** *autonomous-system-number* **Example:** `Router(config-if)# no ipv6 split-horizon eigrp 1`	Disables the sending of IPv6 redirects messages on an interface.
Step 11	**ipv6 dampening-interval eigrp** *autonomous-system-number interval* **Example:** `Router(config-if)# ipv6 dampening-interval eigrp 1 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 12	**router eigrp** *autonomous-system-number* **Example:** `Router(config-if)# router eigrp 1`	Configures the EIGRP address family process and enters router configuration mode.
Step 13	**network** *address* **Example:** `Router(config-router)# network 209.165.200.225`	Configures the a network address.
Step 14	**ipv6 router eigrp** *autonomous-system-number* **Example:** `Router(config-router)# ipv6 router eigrp 1`	Configures EIGRP routing process in IPV6.
Step 15	**end** **Example:** `Router(config-rtr)#end`	(Optional) Exits the current configuration mode and returns to privileged EXEC mode.

Setting the EIGRP Interval-based Dampening Interval for VMI Interfaces using named-style configuration

Perform this task to set an interval-based dampening interval for VMI interfaces using named-style configuration.

Prerequisites

This configuration assumes that a virtual template and appropriate PPPoE configurations have already been completed. Refer to the *Cisco IOS IP Mobility Configuration Guide* for VMI configuration details.

This configuration sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **ip address** *address mask*

5. **no ip redirects**
6. **ipv6 address** *address*
   or
   ipv6 enable
7. **router eigrp** *virtual-instance-name*
8. **address-family ipv4 autonomous-system** *autonomous-system-number*
9. **network** *network-address*
10. **af-interface** *interface-name interface-number*
11. **dampening-interval** *interval*
12. **exit**
13. **exit**
14. **address-family ipv6 autonomous-system** *autonomous-system-number*
15. **af-interface** *interface-name interface-number*
16. **dampening-interval** *interval*
17. **end**

DETAILED STEPS

	Command	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** *interface-type interface-number* **Example:** `Router(config)# interface vmi 1`	Enters interface configuration and creates a VMI interface.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI interface.
Step 5	**no ip redirects** **Example:** `Router(config-if)# no ip redirects`	Prevents the router from sending redirects.

	Command	Purpose
Step 6	**ipv6 address** *address* or **ipv6 enable** **Example:** `Router(config)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address.
Step 7	**router eigrp** *virtual-instance-name* **Example:** `Router(config-if)# router eigrp name`	Enables EIGRP for IPv6 on the interface.
Step 8	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv4 autonomous-system 1`	Enters address-family configuration mode to configure an EIGRP routing instance.
Step 9	**network** *network-address* **Example:** `Router(config-router-af)# network 209.165.200.225`	Configures the network address.
Step 10	**af-interface** *interface-name interface-number* **Example:** `Router(config-router-af)# af-interface vmi 1`	Enters address-family interface configuration mode.
Step 11	**dampening-interval** *interval* **Example:** `Router(config-router-af-interface)# dampening-interval 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 12	**exit** **Example:** `Router(config-router-af-interface)# exit`	Exits the address-family interface configuration mode.
Step 13	**exit** **Example:** `Router(config-router-af)# exit`	Exits the address-family configuration mode and enters the router confiuration mode.
Step 14	**address-family ipv6** *autonomous-system autonomous-system-number* **Example:** `Router(config-router)# address-family ipv6 autonomous-system 1`	Enters address-family configuration mode to configure an EIGRP routing instance for IPv6.
Step 15	**af-interface** *interface-name interface-number* **Example:** `Router(config-router-af)# af-interface vmi 1`	Enters address-family interface configuration mode.

	Command	Purpose
Step 16	**dampening-interval** *interval* **Example:** `Router(config-router-af-interface)# dampening-interval 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 17	**end** **Example:** `Router(config-router-af-interface)# end`	(Optional) Exits the current configuration mode and returns to privileged EXEC mode.

Enabling Multicast Support on a VMI Interface

Perform this task to enable bypass mode on a VMI interface and override the default aggregation that occurs on VMI interfaces.

Prerequistes

This configuration assumes that you have already configured a virtual template and appropriate PPPoE sessions for the VMI interface.

Restrictions

Using bypass mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **mode bypass** command, Cisco recommends that you copy the running configuration to NVRAM because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **mode bypass**
5. **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	**interface** *type number* **Example:** `Router(config-if)# interface vmi1`	Enters interface configuration mode and reates a VMI interface.
Step 4	**mode bypass** **Example:** `Router(config-if)# mode bypass`	Overrides the default aggregation on the VMI interface and sets the mode to bypass to support multicast traffic on the interface.
Step 5	**end** **Example:** `Router(config-if)# exit`	Exits interface configuration.

Creating and Configuring a VMI Interface for OSPFv3

Perform this task to create the VMI interface and associate it with the Ethernet interface on which PPPoE is enabled. When you create a VMI interface, assign the IPv6 or IPv4 address to that VMI interface definition.

Restrictions

Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 cef**
5. **policy-map** *policy-map-name*
6. **class class-default**
7. **fair-queue**
8. **interface virtual-template** *number*
9. **ipv6 enable**

10. **no keepalive**
11. **service-policy output** *policy-name*
12. **interface** *interface-type interface-number*
13. **ipv6 enable**
14. **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]
15. **ipv6 ospf network point-to-multipoint**
16. **ipv6 ospf cost dynamic hysteresis** [**threshold** *threshold-value*]
17. **ipv6 ospf cost dynamic weight throughput** *percent*
18. **ipv6 ospf cost dynamic weight resources** *percent*
19. **ipv6 ospf cost dynamic weight latency** *percent*
20. **ipv6 ospf cost dynamic weight L2-factor** *percent*
21. **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]
22. **physical-interface** *interface-type/slot*
23. **ipv6 router ospf** 1
24. **router-id** *ip-address*
25. **redistribute connected** *metric-type 1*
26. **timers spf** *spf-delay spf-hold*
27. **end**

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 unicast-routing`
	
	Example:
	`Router(config)# ipv6 unicst-routing`
		Enables IPv6 unicast routing.

Step 4	**`ipv6 cef`** **Example:** `Router(config)# ipv6 cef`	Enables IPv6 CEF on the router.

	Command or Action	Purpose
Step 5	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map fair-queue`	Enters policy map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 6	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
Step 7	**fair-queue** **Example:** `Router(config-pmap)# fair-queue`	Enables weighted fair queueing (WFQ) on the interface
Step 8	**interface virtual-template** *number* **Example:** `Router(config-if)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 9	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 on the virtual template.
Step 10	**no keepalive** **Example:** `Router(config-if)# no keepalive`	Turns off PPP keepalive messages.
Step 11	**service-policy output** *policy-name* **Example:** `Router(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config-if)# interface vmi 1`	Creates a VMI interface.
Step 13	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 routing on the VMI interface.
Step 14	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **Example:** `Router(config-if)# ipv6 ospf 1 area 0`	Enables IPv6 OSPF routing on the interface.

	Command or Action	Purpose
Step 15	**ipv6 ospf network point-to-multipoint** **Example:** `Router(config-if)# ipv6 ospf network point-to-multipoint`	Specifies the OSPF network type.
Step 16	**ipv6 ospf cost hysteresis** [**threshold** *threshold-value*] **Example:** `ipv6 ospf cost hysteresis threshold 1000`	Sets the hysterisis tolerance for the interface.
Step 17	**ipv6 ospf cost dynamic weight throughput** *percent* **Example:** `Router(config-if)# ipv6 ospf cost dynamic weight throughput 0`	Sets the metric for the throughput threshold.
Step 18	**ipv6 ospf cost dynamic weight resources** *percent* **Example:** `Router(config-if)# ipv6 ospf cost dynamic weight resources 29`	Sets the metric for the resource factor.
Step 19	**ipv6 ospf cost dynamic weight latency** *percent* **Example:** `Router(config-if)# ipv6 ospf cost dynamic weight latency 29`	Sets the threshold for the latency factor.
Step 20	**ipv6 ospf cost dynamic weight L2-factor** *percent* **Example:** `Router(config-if)# ipv6 ospf cost dynamic weight L2-factor 29`	Sets the metric for the Layer 2 -to- Layer 3 delay factor.
Step 21	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **Example:** `Router(config-if)# ipv6 ospf 1 area 0`	Enables OSPF for IPv6 on an interface.
Step 22	**physical-interface** *interface-type/slot* **Example:** `Router(config-if)# physical-interface FastEthernet 0/1`	Creates the physical subinterface to be associated with the VMI interfaces on the router.
Step 23	**ipv6 router ospf** *process-id* ***Example:*** `Router(config-if)# ipv6 router ospf 1`	Enables OSPF for IPv6 router configuration mode.

	Command or Action	Purpose
Step 24	**router-id** *ip-address* **Example:** `Router(config-rtr)# router-id 10.1.1.1`	Identifies a specific router rather than allowing the dynamic assignment of the router to occur.
Step 25	**redistribute connected metric-type 1** **Example:** `Router(config-rtr)# redistribute connected metric-type 1`	Redistributes IPv6 routes from one routing domain into another routing domain. Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
Step 26	**timers spf** *spf-delay spf-hold* **Example:** `Router(config-rtr)#timers spf 1 1`	Specifies the spf delay time and maximum hold time in milliseconds to delay the calculations for Value ranges for these arguments is 1 to 600,000 milliseconds. The OSPF Shortest Path First Throttling feature makes it possible to configure SPF scheduling in millisecond intervals and to potentially delay shortest path first (SPF) calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology
Step 27	**end** **Example:** `Router(config-rtr)# end`	(Optional) Exits the router configuration mode and returns to privileged EXEC mode.

Example

The following shows a sample output display to verify the OSPF Cost Dynamic for a VMI.

```
Router1# show ipv6 ospf interface serial2/0

Serial2/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 200.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

Verifying the VMI Configuration

Possible commands to use in verifying the configuration include:

- show pppoe session all
- show interface vmi

- show vmi neighbors
- show vmi neighbors detail
- show ip eigrp interfaces
- show ip eigrp neighbors
- show ipv6 eigrp interfaces
- show ipv6 eigrp neighbors
- show ipv6 ospf interface

Configuration Examples for VMI PPPoE

Basic VMI PPPoE Configuration with EIGRP IPv4: Example

This example illustrates the simplest configuration using EIGRP as the routing protocol. This configuration includes one VMI interface.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password test
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
```

```
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
```

```
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.226 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
!
interface vmi1
 ip address 209.165.200.226 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
dampening-change 50
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Basic VMI PPPoE Configuration Using EIGRP for IPv6: Example

This example shows the basic requirements for configuring a VMI interface that uses EIGRP for IPv6 as the routing protocol. It includes one VMI interface.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
ip cef
!
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
!
!
archive
 log config
!
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
!
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
!
interface Loopback1
```

```
 ip address 209.165.200.226 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
```

```
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 physical-interface FastEthernet0/0
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

VMI PPPoE Configuration Using EIGRP for IPv4 and IPv6: Example

The following examples shows how to configure VMI PPPoE using EIGRP as the IP routing protocol when you have both IPv4 and IPv6 addresses configured on the interface. This configuration includes one VMI interface.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
```

```
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
```

```
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 ip address 209.165.200.225 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
dampening-interval 30
```

```
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.225 255.255.255.224
 network 209.165.200.226 255.255.255.224
 auto-summary
!
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

EIGRP Metric Dampening for VMI Interfaces: Examples

The **dampening-change** and **dampening-interval** commands are supported only for Mobile Ad Hoc Networking (MANET) router-to-radio links.

Dampening-change command

When a peer metric changes on an interface that is configured with the **dampening-change** command, EIGRP multiplies the dampening-change percentage with the old peer metric and compares the result (the threshold) to the difference between the old and new metrics. If the metric difference is greater than the calculated threshold, then the new metric is applied and routes learned from that peer are updated and advertised to other peers. If the metric difference is less than the threshold, the new metric is discarded.

There are exceptions that will result in an immediate update regardless of the dampening-change setting:

- An interface is down.
- A route is down.
- A change in metric which results in the router selecting a new next hop.

Peer metric changes that do not exceed a configured change percentage and that do not result in a routing change do not result in an update being sent to other adjacencies. Peer metric changes are based on the stored last-update of the peer. Peer metric changes that exceed the threshold value are stored and used for future comparisons.

The **dampening-interval** command is supported only in Mobile Ad Hoc Networking (MANET) Router-to-Radio links.

Dampening-interval command

When a peer metric changes on an interface that is configured with a dampening interval, EIGRP will apply the metric change only if the time difference since the last metric changed exceeds the specified interval. If the time difference is less than the specified interval, the update is discarded.

There are exceptions that result in an immediate update regardless of the dampening interval settings:

- An interface is down.
- A route is down.

A change in metric that results in the router selecting a new next hop.

EIGRP Change-based Dampening for VMI Interfaces: Example

The following example configures EIGRP address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 5400
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# dampening-interval 45
```

EIGRP Interval-based Dampening for VMI Interfaces: Example

The following example configures EIGRP address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 5400
Router(config-router-af)# af-interface ethernet0/0
```

VMI PPPoE Configuration for OSPFv3: Example

The following example shows how to configure VMI PPPoE using OSPFv3 as the routing protocol. This configuration includes three VMI interfaces.

```
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
!
!
ip cef
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host2
 pppoe service manet_radio
!
!
```

```
multilink bundle-name authenticated
no virtual-template subinterface
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host2
!
bba-group pppoe VMI2
 virtual-template 2
 service profile host2
!
bba-group pppoe VMI3
 virtual-template 3
 service profile host2
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 load-interval 30
 duplex full
 speed 100
 pppoe enable group VMI3
!
interface GigabitEthernet0/0
 no ip address
 load-interval 30
 duplex full
 speed 100
 pppoe enable group VMI1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 load-interval 30
 duplex full
 speed 100
 pppoe enable group VMI2
!
interface Serial1/0
 no ip address
 shutdown
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
```

```
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Virtual-Template3
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
!
interface Vlan503
 ip address 10.2.2.2 255.255.255.0
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface vmi1
 no ip address
```

```
 load-interval 30
ipv6 enable
 ipv6 ospf network point-to-multipoint
 ipv6 ospf cost dynamic hysteresis threshold 1000
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
 ipv6 ospf 1 area 0
 physical-interface GigabitEthernet0/0
!
interface vmi2
 no ip address
 load-interval 30
ipv6 enable
 ipv6 ospf network point-to-multipoint
 ipv6 ospf cost dynamic hysteresis threshold 1000
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
 ipv6 ospf 1 area 0
 physical-interface GigabitEthernet0/1
!
interface vmi3
 no ip address
 load-interval 30
ipv6 enable
 ipv6 ospf network point-to-multipoint
 ipv6 ospf cost dynamic hysteresis threshold 1000
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
 ipv6 ospf 1 area 0
 physical-interface FastEthernet0/0
!
!
!
no ip http server
no ip http secure-server
!
ipv6 router ospf 1
 router-id 10.16.1.1
 log-adjacency-changes
 redistribute connected metric-type 1
 timers spf 1 1

!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

```
end
```

VMI PPPoE Configuration Using Multiple Virtual Templates: Example

The following example shows how to configure VMI using multiple virtual templates. This example shows two VMIs, each with a different service name.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
!
subscriber profile router1_ground
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
```

```
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
```

```
!
interface Virtual-Template2
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.225 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Enabling Multicast Support on a VMI Interface: Examples

Bypass Mode on VMI Interfaces

Enabling Multicast on VMI interfaces includes changing the VMI interface to bypass mode and enabling Protocol Independent Multicast (PIM) sparse mode on the virtual-template interface.

```
Router# enable
Router# configure terminal
!
Router(config)# interface Virtual-Template1
Router(config-if)#ip address 209.165.200.227 255.255.255.224
Router(config-if)# load-interval 30
Router(config-if)# no keepalive
Router(config-if)# ip pim sparse-dense-mode
Router(config-if)# service-policy output FQ
!
!
Router(config)# interface vmi1
```

```
Router(config-if)# ip address 10.3.9.1 255.255.255.0
Router(config-if)# load-interval 30
Router(config-if)# physical-interface FastEthernet0/0
Router(config-if)# mode bypass
!
Router(config)# end
```

OSPF v3 Using Bypass Mode for IPv6 Multicast Traffic Example

The **ipv6 ospf network point-to-multipoint** command in this OSPF example is needed to allow OSPFv3 to learn dynamic metrics from the link.

```
version 12.4
!
hostname host1
!
enable
configure terminal
!
no aaa new-model
clock timezone EST -5
!
!
!
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
interface Loopback1
 no ip address
 load-interval 30
 ipv6 address 2001:0DB1::1/64
 ipv6 enable

pv6 ospf 1 area 0
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 ipv6 enable
 pppoe enable group VMI1
```

```
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
!
ipv6 ospf network point-to-multipoint
ipv6 ospf cost dynamic
 ipv6 ospf 1 area 0
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 no ip address
 no ip mroute-cache
load-interval 30
 ipv6 address 2001:0DB8::/32
```

```
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Vlan503
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet0/0
 mode bypass
!
!
no ip http server
no ip http secure-server
!ipv6 router ospf 1
 log-adjacency-changes
 redistribute connected metric-type 1
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

EIGRP IPv4 with Bypass Mode Example

In this example, the IP address of the VMI1 interface needs to be defined, but it will not be routable because the vmi interface will be configured as down/down.

```
ostname host1
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
```

```
 class class-default
  fair-queue
!
!
!bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
ip address 209.165.200.225 255.255.255.224
 load-interval 30
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
shutdown
 clock rate 2000000
!
interface Serial1/3
no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip address 209.165.200.225 255.255.255.224
```

```
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
ipv6 enable
!
interface vmi1
ip address 209.165.200.226 255.255.255.224
 load-interval 30
 physical-interface FastEthernet0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 209.165.200.225 255.255.255.224
 network 209.165.200.226 255.255.255.224
```

EIGRP for IPv6 Example

```
version 12.4
enable
configure terminal

ip cef
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
!
archive
 log config
!
!
policy-map FQ
class class-default
 fair-queue
!
!
!
```

```
bba-group pppoe VMI1
 virtual-template 1
service profile host1
!
!
interface Loopback1
load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown

clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
```

```
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 no ip address
 no ip mroute-cache
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface Vlan503
 no ip address
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
no ip address
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet0/0
 mode bypass
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 no shutdown
 redistribute connected
!
!
!
```

EIGRP with IPv4 and IPv6 Traffic Using Bypass Mode Example

```
version 12.4T
!
hostname host1
!
enable
configure terminal

ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
no virtual-template subinterface
```

```
!
archive
 log config
!
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
```

```
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.226 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 eigrp router-id 10.9.1.1
 no shutdown
 redistribute connected
!
!
!
end
```

PPPoE Configuration: Example

In the following example, the subscriber profile uses a predefined string manet_radio to determine whether an inbound PPPoE session is coming from a device that supports VMI. All IP definitions are configured on the VMI interface rather than on the FastEthernet or Virtual-Template interfaces; when those interfaces are configured, do not specify either an IP address or an IPv6 address.

No IP address is specified and IPv6 is enabled by default on the VMI interface.

```
subscriber profile list1
  pppoe service service1
  subscriber authorization enable

!
bba-group pppoe bba1
  virtual-template 1
  service profile list1
!
interface FastEthernet0/1
  no ip address
  pppoe enable group bba1
!
interface Virtual-Template 1
  no ip address
  no peer default ip-address
!
interface vmi 1
  no ip address
  physical-interface FastEthernet0/1
```

Configuring Two VMIs: Example

The following example shows a configuration that includes two VMIs, each having different service names.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
!
subscriber profile router1_ground
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
```

```
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
 policy-map FQ
 class class-default
 fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 ip unnumbered vmi2
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.226 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.227 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
```

```
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Marking and Queuing Packets over VMI: Example

This configuration example includes QoS features in use with a VMI. Packets are marked either outbound or inbound over the VMI according to a policy map defined on the interface. This configuration differs slightly from standard QoS configurations because it requires that two different policies be applied to two different interfaces.

You apply the fair queue policy to the virtual template to define the queueing mechanism. To mark packets, you create a another policy and apply it to VMI to mark the traffic. The two policy maps work in tandem to provide the QoS support on the radio interface

Note Packets will not be marked if you use the standard fair queue class or use hierarchical policy maps applied to the virtual templates.

The examples that follow show the device configurations that support the marking and queueing on a VMI.

Output Configuration of VMI and Policy Map Configured on Router 1

```
!
!
!
class-map match-all udp-traffic
 match access-group 100
!
!
policy-map FQ
 class class-default
  fair-queue
policy-map my-marker
 class udp-traffic
  set dscp af41
!
!
interface Virtual-Template1
.
.
.
 service-policy output FQ
!
!
interface vmi1
.
.
.
 service-policy output my-marker
.
```

```
.
.
!
access-list 100 permit udp any any
!
```

Input Configuration for VMI and Policy Map configured on Router 2

```
!
!
!
class-map match-all udp-traffic
 match access-group 100
!
!
policy-map FQ
 class class-default
  fair-queue
policy-map my-marker
 class udp-traffic
  set dscp ef
!
interface Virtual-Template1
...
 service-policy output FQ
!
interface vmi1
...
 service-policy input my-marker
!
access-list 100 permit udp any any
!
```

This display is output from the **show policy-map** command for the VMI and policy map configured on on Router 1.

```
Router1# show policy-map int vmi1

 vmi1

  Service-policy output: my-marker

    Class-map: udp-traffic (match-all)
      5937331 packets, 6234197550 bytes
      30 second offered rate 840000 bps, drop rate 0 bps
      Match: access-group 100
      QoS Set
        dscp af41
          Packets marked 5937331

    Class-map: class-default (match-any)
      12829 packets, 769740 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
!
!
!
```

This display is output from the **show policy-map** command for the VMI and policy map configured on on Router 2.

```
Router2# show policy-map int vmi1
```

```
vmi1

 Service-policy input: my-marker

   Class-map: udp-traffic (match-all)
     5971417 packets, 6150560540 bytes
     30 second offered rate 824000 bps, drop rate 0 bps
     Match: access-group 100
     QoS Set
       dscp ef
         Packets marked 5971418

   Class-map: class-default (match-any)
     26167 packets, 1623087 bytes
     30 second offered rate 0 bps, drop rate 0 bps
     Match: any
```

Additional References

The following sections provide references related to Mobile Ad Hoc Networks for Router-to-Radio Communications.

Related Documents

Related Topic	Document Title
EIGRP	• *Cisco IOS IP Routing Protocols Configuration Guide* • *Cisco IOS IP Routing Protocols Command Reference*
OSPF	• *Cisco IOS IP Routing Protocols Configuration Guide* • *Cisco IOS IP Routing Protocols Command Reference*
PPPoE	• *Cisco IOS Dial Solutions Configuration Guide* • *Cisco IOS Dial Solutions Command Reference*
IPv6	• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*
Implementing IPv6 Addressing and Basic Connectivity	*Cisco IOS IPv6 Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIB 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

RFC	Title
RFC-2373	IP Version 6 Addressing Architecture
RFC-2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC-4938	PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information About the Mobile Ad Hoc Networks for Router-to-Radio Communications

Table 7 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(14)T or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 7 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 7 Feature Information for Mobile Ad Hoc Networks for Router-to-Radio Communications

Feature Name	Releases	Feature Information
PPPoE Support for Credit Flow and Metrics on Router-to-Radio Links Feature	12.4(15)XF 12.4(15)T 15.0(1)M	Credit-based flow control provides in-band and out-of-band credit grants in each direction. Link Quality Metrics are used to report link performance statistics that are then used to influence routing. The following sections provide information about this feature: • PPPoE Interfaces for Mobile Radio Communications, page 4 • PPPoE Credit-based Flow Control, page 13 • Configuration Examples for VMI PPPoE, page 43 The following commands were introduced or modified: **show pppoe session, show vmi neighbors, show pppoe session**

Table 7 Feature Information for Mobile Ad Hoc Networks for Router-to-Radio Communications

Feature Name	Releases	Feature Information
OSPFv3 Dynamic Interface Cost Support	12.4(15)XF 12.4(15)T 15.0(1)M	OSPFv3 Dynamic Interface Cost Support provides enhancements to the OSPFv3 cost metric for supporting Mobile Ad Hoc Networking. The following section provides information about this feature; • OSPF Cost Calculation for VMI Interfaces, page 6 The following commands were introduced or modified: **ipv6 ospf cost, debug ipv6 ospf l2api, test ospfv3 interface** ***name***
EIGRP L2/L3 API and Tunable Metric for Mobile Ad Hoc Networks	12.4(15)XF 12.4(15)T 15.0(1)M	EIGRP uses dynamic raw radio link characteristics (current and maximum bandwidth, latency, and resources) to compute a composite EIGRP metric. A tunable Hysteresis mechanism helps to avoid churn in the network as a result of the change in the link characteristics. In addition to the link characteristics, the L2L3 API provides an indication when a new adjacency is discovered, or an existing unreachable adjacency is again reachable. When EIGRP receives the adjacency signals, it responds with an immediate Hello out the specified interface to expedite the discovery of the EIGRP peer. The following section provides information about this feature: • Link Quality Metrics Reporting for OSPFv3 and EIGRP with VMI Interfaces, page 5 • Basic VMI PPPoE Configuration Using EIGRP for IPv6: Example, page 46 • VMI PPPoE Configuration Using EIGRP for IPv4 and IPv6: Example, page 48 The following commands were introduced or modified: **dampening-change, dampening-interval, debug eigrp notifications, debug vmi**