Cisco IOS Mobile Wireless Home Agent Configuration Guide

Release 12.4

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS Mobile Wireless Home Agent Configuration Guide
© 2008 Cisco Systems, Inc. All rights reserved.

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS 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, page i
- Audience, page i
- Documentation Conventions, page ii
- Documentation Organization, page iii
- Additional Resources and Documentation Feedback, page xi

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 i ntended 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 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 includes the following topics:

- Typographic Conventions, page ii
- Command Syntax Conventions, page ii
- Software Conventions, page iii
- Reader Alert Conventions, page iii

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.
|	A vertical line, called a pipe, 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 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

The Cisco IOS documentation set 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. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- 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

Cisco IOS documentation 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 severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not 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 informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers 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 documentation organization 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 describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided 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/all_release/all_mcl.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 and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE 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.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

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.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS AppleTalk Configuration Guide *Cisco IOS XE 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 and Cisco IOS XE 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 and DSL Configuration Guide *Cisco IOS XE Broadband and DSL Configuration Guide* *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (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 operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS XE 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 XE DECnet Configuration Guide* *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS XE 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), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Configuration Guide *Cisco IOS XE 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).
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS XE 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 XE 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 XE 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 XE 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).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS XE IP Routing Protocols Configuration Guide* *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS XE 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 XE 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 XE IPv6 Configuration Guide* *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS XE ISO CLNS Configuration Guide* *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS XE 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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Multiprotocol Label Switching Configuration Guide *Cisco IOS XE 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 XE NetFlow Configuration Guide* *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, export features.
Cisco IOS Network Management Configuration Guide *Cisco IOS XE 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 XE 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, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
Cisco IOS Quality of Service Solutions Configuration Guide *Cisco IOS XE Quality of Service Solutions Configuration Guide* *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
Cisco IOS Security Configuration Guide *Cisco IOS XE Security Configuration Guide* *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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
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* *Cisco IOS XE 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, refer to 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 XE 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 XE Wide-Area Networking Configuration Guide* *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), 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 Cisco IOS Supplementary Documents and Resources

Document Title	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 Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the 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 at the following URL: http://www.cisco.com/go/mibs
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 published 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.

Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

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

- Initially Configuring a Device, page i
- Using the CLI, page ii
- Saving Changes to a Configuration, page xii
- Additional Information, page xii

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 and Cisco IOS XE 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 Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

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 ASR1000 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, page ii
- Using the Interactive Help Feature, page v
- Understanding Command Syntax, page vi
- Understanding Enable and Enable Secret Passwords, page viii
- Using the Command History Feature, page viii
- Abbreviating Commands, page ix
- Using Aliases for CLI Commands, page ix
- Using the no and default Forms of Commands, page x
- Using the debug Command, page x
- Filtering Output Using Output Modifiers, page x
- Understanding CLI Error Messages, page xi

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 the Cisco ASR1000 series router)	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 using 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 possibly 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 how to use the Help feature.

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

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 number. 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 number 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 CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved 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 CLI 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 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_book.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** and **default** forms of commands are described in the command pages of command references.

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 and Cisco IOS XE 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.

Three output modifiers are available and are described as follows:

- **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 documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

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

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- 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\

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.

CHAPTER 1

Overview of the Cisco Mobile Wireless Home Agent

This chapter illustrates the functional elements in a typical CDMA2000 packet data system, the Cisco products that are currently available to support this solution. and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

- Feature Overview, page 1-1
- System Overview, page 1-2
- Cisco Home Agent Network, page 1-3
- Packet Data Services, page 1-4
- Features, page 1-7
- Benefits, page 1-9
- The Home Agent, page 1-9

Feature Overview

Cisco's Mobile Wireless Packet Data Solution includes the Packet Data Serving Node (PDSN) with Foreign Agent (FA) functionality, the Cisco Mobile Wireless Home Agent (HA), Authentication, Authorization and Accounting (AAA) servers, and several other security products and features. The solution is standards compliant, and is designed to meet the needs of the mobile wireless industry as it transitions towards third-generation cellular data services.

The Home Agent is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic sent to the terminal is routed through the Home Agent. With reverse tunneling, traffic from the terminal is also routed through the Home Agent.

A PDSN provides access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations using a Code Division Multiple Access 2000 (CDMA2000) Radio Access Network (RAN). The Cisco PDSN is a Cisco IOS software feature that runs on Cisco 7200 routers, Catalyst 6500 switches, and Cisco 7600 Internet routers, and acts as an access gateway for Simple IP and Mobile IP stations. It provides FA support and packet transport for virtual private networking (VPN). It also acts as a AAA client.

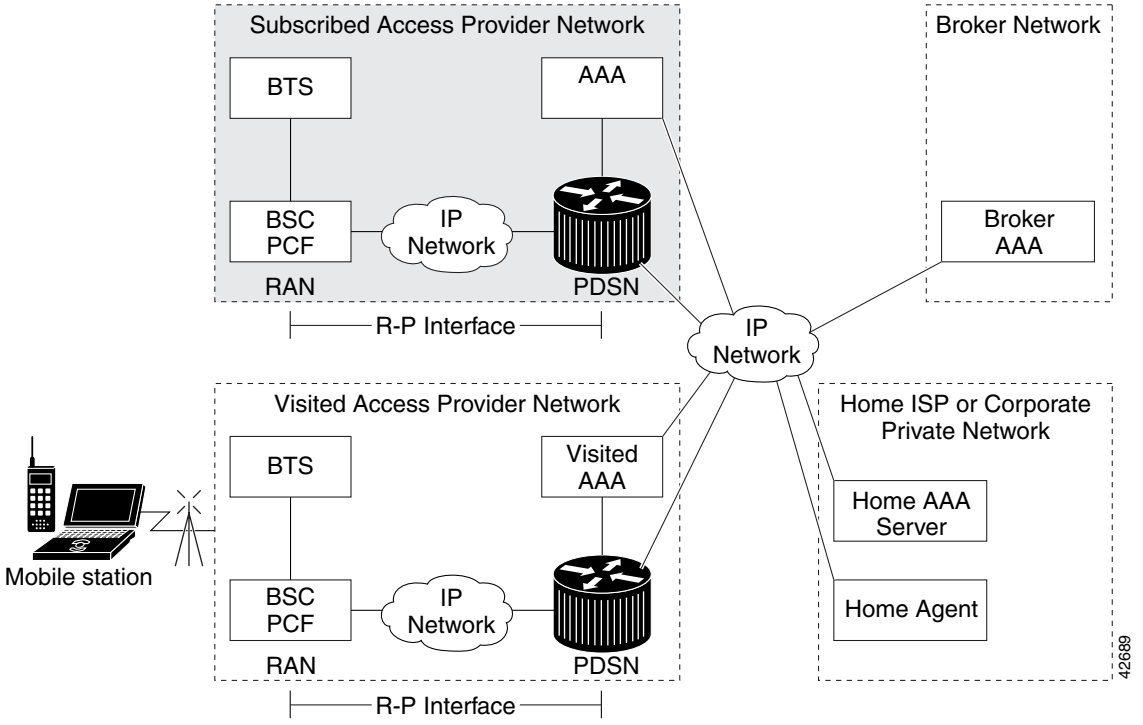
The Cisco PDSN and the Cisco Home Agent support all relevant 3GPP2 standards, including those that define the overall structure of a CDMA2000 network, and the interfaces between radio components, the Home Agent, and the PDSN.

System Overview

CDMA is one of the standards for mobile communication. A typical CDMA2000 network includes terminal equipment, mobile termination, base transceiver stations (BTSs), base station controllers (BSCs), PDSNs, and other CDMA network and data network entities. The PDSN is the interface between a BSC and a network router.

Figure 1-1 illustrates the relationship of the components of a typical CDMA2000 network, including a PDSN and a Home Agent. In this illustration, a roaming mobile station user is receiving data services from a visited access provider network, rather than from the mobile station user's subscribed access provider network.

Figure 1-1 The CDMA Network



As the illustration shows, the mobile station, which must support either Simple IP or Mobile IP, connects to a radio tower and BTS. The BTS connects to a BSC, which contains a component called the Packet Control Function (PCF). The PCF communicates with the Cisco PDSN through an A10/A11 interface. The A10 interface is for user data and the A11 interface is for control messages. This interface is also known as the RAN-to-PDSN (R-P) interface. For the Cisco Home Agent Release 2.1 and above, you must use a Fast Ethernet (FE) interface as the R-P interface on the Cisco 7200 platform, and a Giga Ethernet (GE) interface on the Cisco Multi-Processor WAN Application Module (MWAM) platform.

The IP networking between the PDSN and external data networks is through the PDSN-to-intranet/Internet (P_i) interface. For the Cisco Home Agent, you can use either an FE or GE interface as the P_i interface.

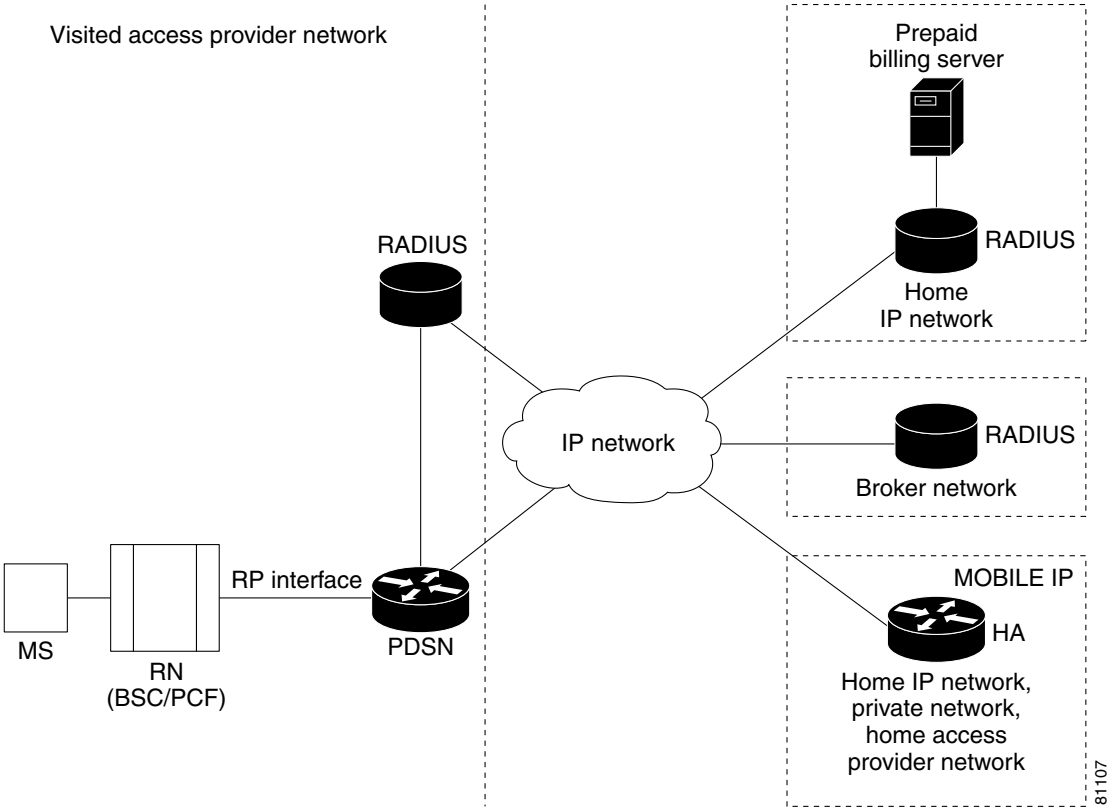
For "back office" connectivity, such as connections to a AAA server, the interface is media independent. Any of the interfaces supported on the Cisco 7206 can be used to connect to these types of services, but we recommend that you use either an FE or GE interface as the P_i interface.

Cisco Home Agent Network

Figure 1-2 illustrates the functional elements in a typical CDMA2000 packet data system, and Cisco products that are currently available to support this solution. The Home Agent, in conjunction with the PDSN and Foreign Agent, allows a mobile station with Mobile IP client function, to access the Internet or corporate intranet using Mobile IP-based service access. Mobile IP extends user mobility beyond the coverage area of the current, serving PDSN/Foreign Agent. If another PDSN is allocated to the call (following a handoff), the target PDSN performs a Mobile IP registration with the Home Agent; this ensures that the same home address is allocated to the mobile station. Additionally, clients without a Mobile IP client can also make use of these services by using the Proxy Mobile IP capability provided by the PDSN.

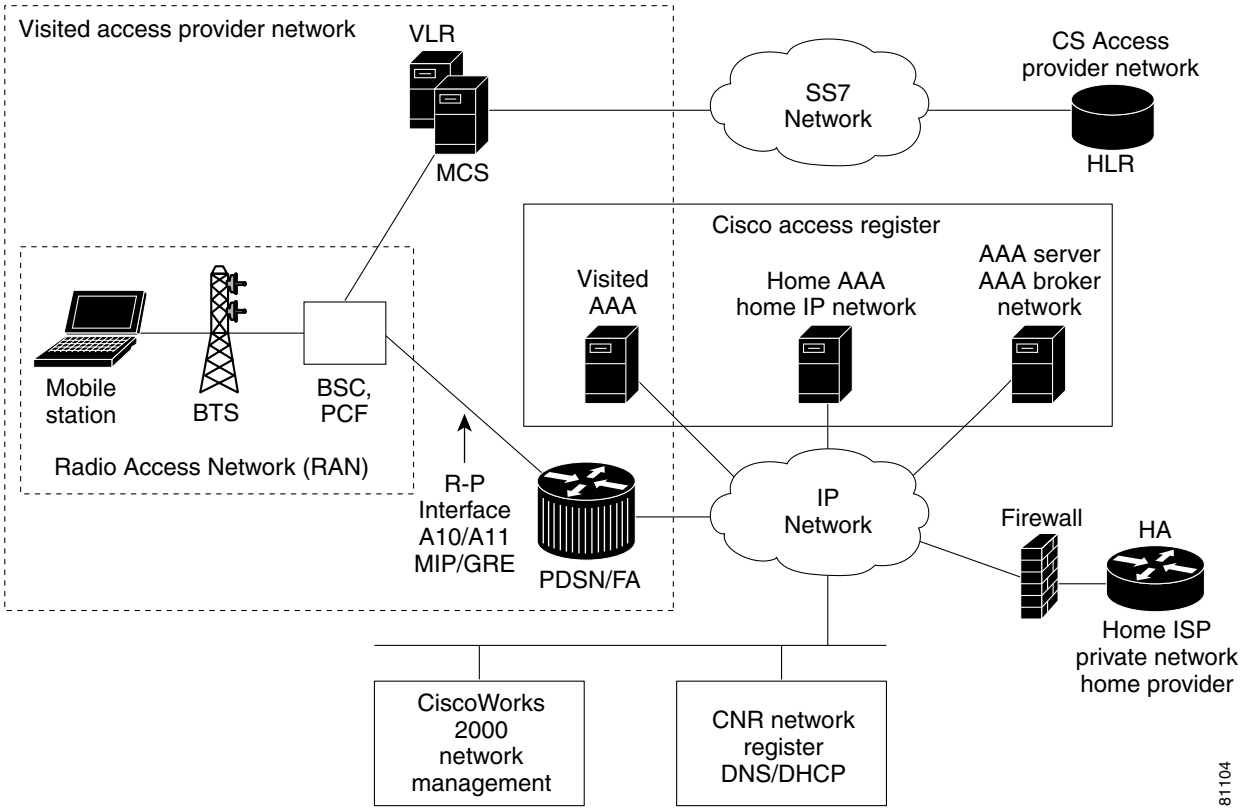
The Home Agent, then, is the anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. Traffic is routed through the Home Agent, and the Home Agent also provides Proxy ARP services. In the case of reverse tunneling, traffic from the terminal is also routed through the Home Agent.

Figure 1-2 Cisco Products for CDMA2000 Packet Data Services Solution



For Mobile IP services, the Home Agent would typically be located within an ISP network, or within a corporate domain. However, many ISPs and/or corporate entities may not be ready to provision Home Agents by the time service providers begin rollout of third-generation packet data services. As a remedy, Access service providers could provision Home Agents within their own domains, and then forward packets to ISPs or corporate domains using VPDN services. Figure 1-3 illustrates the functional elements that are necessary to support Mobile IP-based service access when the Home Agent is located in the service provider domain.

Figure 1-3 Cisco Mobile IP-Based Service Access With Home Agent in Service Provider Network



For Mobile IP and Proxy-Mobile IP types of access, these solutions allow a mobile user to roam within and beyond its service provider boundaries, while always being reachable and addressable through the IP address assigned on initial session establishment. Details of Mobile IP and Proxy Mobile IP Services can be found in the Packet Data Services section that follows.

Packet Data Services

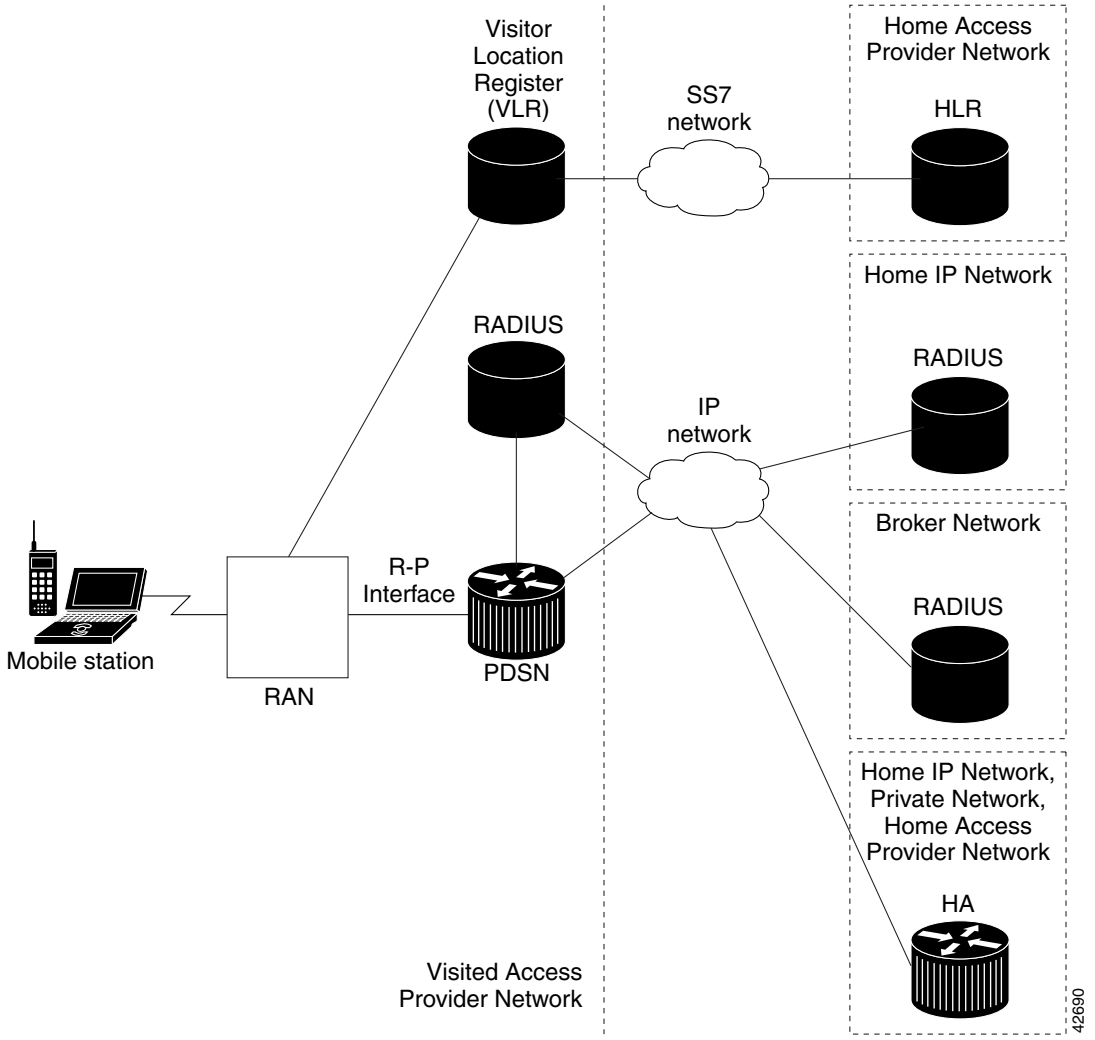
In the context of a CDMA2000 network, the Cisco Home Agent supports two types of packet data services: Mobile IP and Proxy Mobile IP services. From the perspective of the Cisco Home Agent, these services are identical.

Cisco Mobile IP Service

With Mobile IP, the mobile station can roam beyond the coverage area of a given PDSN and still maintain the same IP address and application-level connections.

Figure 1-4 shows the placement of the Cisco Home Agent in a Mobile IP scenario.

Figure 1-4 CDMA Network—Mobile IP Scenario



The communication process occurs in the following order:

1. The mobile station registers with its Home Agent (HA) through an FA. In the context of the CDMA2000 network, the FA is the Cisco PDSN.
2. The Cisco HA accepts the registration, assigns an IP address to the mobile station, and creates a tunnel to the FA. The resulting configuration is a PPP link between the mobile station and the FA (or PDSN), and an IP-in-IP or GRE tunnel between the FA and the HA.

   As part of the registration process, the Cisco HA creates a binding table entry to associate the mobile station's home address with its *Care-of* Address (CoA).

Note While away from home (from the HA's perspective), the mobile station is associated with a care-of address. This address identifies the mobile station's current, topological point of attachment to the Internet, and is used to route packets to the mobile station. Either a Foreign Agent's address, or an address obtained by the mobile station for use while it is present on a particular network, is used as the care-of address. In the case of the Cisco Home Agent, the care-of address is always an address of the Foreign Agent.

3. The HA advertises network reachability to the mobile station, and tunnels datagrams to the mobile station at its current location.
4. The mobile station sends packets with its home address as the source IP address.
5. Packets destined for the mobile station go through the HA, which tunnels them to the PDSN. From there they are sent to the mobile station using the care-of address. This scenario also applies to reverse tunneling, which allows traffic moving from the mobile to the network to pass through the Home Agent.
6. When the PPP link is handed off to a new PDSN, the link is renegotiated and the Mobile IP registration is renewed.
7. The HA updates its binding table with the new care-of address.

Note For more information about Mobile IP, refer to the Cisco IOS Release 12.3 documentation modules *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command Reference.* RFC 2002 describes the specification in detail. TIA/EIA/IS-835-B also defines how Mobile IP is realized in the Home Agent.

Cisco Proxy Mobile IP Service

While PPP, which is widely used to connect to an Internet Service Provider (ISP), is ubiquitous in IP devices, certain service providers lack commercially available Mobile IP client software. As an alternative to Mobile IP, you can use Cisco's Proxy Mobile IP feature. This capability of the Cisco PDSN, which is integrated with PPP, enables the PDSN (functioning as a Foreign Agent) and a Mobile IP client, to provide mobility to authenticated PPP users.

The communication process occurs in the following order:

1. The Cisco PDSN (acting as an FA) collects and sends mobile station authentication information to the AAA server (specifically, PPP authentication information).
2. If the mobile station is successfully authorized to use Cisco PDSN Proxy Mobile IP service, the AAA server returns the registration data and an HA address.
3. The FA uses this information, and other data, to generate a registration request (RRQ) on behalf of the mobile station, and sends it to the Cisco HA.
4. If the registration is successful, the Cisco HA sends a registration reply (RRP) that contains an IP address to the FA.
5. The FA assigns the IP address (received in the RRP) to the mobile station, using IP control protocol (IPCP).
6. A tunnel is established between the Cisco HA and the FA, or PDSN. If reverse tunneling is enabled, the tunnel carries traffic to and from the mobile station.

Note The PDSN takes care of all Mobile IP re-registrations on behalf of the Proxy-MIP client.

Features

New Features in IOS Release 12.3(14)YX1

This section lists features that were introduced or modified in Home Agent Release 12.3(14)YX1:

- Mobile Equipment Identifier (MEID) Support

This section describes features that were introduced or modified in Home Agent Release 3.0:

- Home Agent Accounting Enhancements
  - Home Agent Accounting in a Redundant Setup
  - Packet count and Byte count in Accounting Records
  - Additional Attributes in the Accounting Records
  - Additional Accounting Methods—Interim Accounting is Supported.
- VRF Mapping on the RADIUS Server
- Conditional Debugging Enhancements
- Home Agent Redundancy Enhancements
  - Geographical Redundancy
  - Redundancy with Radius Downloaded Pool Names
- SNMP Traps to Track Utilization of Local IP Pool
- Support for Supervisor 720 and 1GB MWAM in Supported Platforms
- Mobile-User ACLs in Packet Filtering
- IP Reachability
- DNS Server Address Assignment
- Mobile IP MIB Enhancements in SNMP, MIBs and Network Management

This section lists features that were introduced or modified in previous releases of the Cisco Mobile Wireless Home Agent:

- Mobile IPv4 Registration Revocation, page 7-1
- HA Server Load Balancing, page 6-1
- Home Agent Accounting, page 11-1
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE), page 4-2
- VRF Support on HA, page 12-1
- Hot-lining, page 13-1
- Radius Disconnect, page 7-4
- Conditional Debugging, page 15-3
- Home Address Assignment, page 3-1
- Home Agent Redundancy, page 5-1
- Virtual Networks, page 5-6
- On-Demand Address Pool (ODAP), page 3-6

- Mobile IP IPSec, page 10-2
- Support for ACLs on Tunnel Interface, page 14-1
- Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY, page 14-3
- 3 DES Encryption, page 10-1
- User Profiles, page 14-3
- Mobility Binding Association, page 14-4
- User Authentication and Authorization, page 4-1
- HA Binding Update, page 14-4
- Per User Packet Filtering, page 9-1
- Security, page 10-1

Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7200 series router, Cisco 6500 series switch, or Cisco 7600 series router, configured as a Home Agent, supports the following Home Agent-specific features:

- Support for static IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Support for dynamic IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Multiple flows for different Network Access Identifiers (NAIs) using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge extensions in RFC 3012 - bis 03
  - Mobile IP Agent Advertisement Challenge Extension
  - MN-FA Challenge Extension
  - Generalized Mobile IP Authentication Extension, which specifies the format for the MN-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
  - MN-HA Authentication Extension
  - FA-HA Authentication Extension
- Reverse Tunneling, RFC 2344
- Mobile NAI Extension, RFC 2794
- Multiple tunneling modes between FA and HA
  - IP-in-IP Encapsulation, RFC 2003
  - Generic Route Encapsulation, RFC 2784
- Binding Update message for managing stale bindings
- Home Agent redundancy support

- Mobile IP Extensions specified in RFC 3220
  - Authentication requiring the use of SPI. section 3.2
- Support for Packet Filtering
  - Input access lists
  - Output access lists
- Support for proxy and gratuitous ARP
- Mobile IP registration replay protection using time stamps. Nonce-based replay protection is not supported.

Benefits

The Cisco Mobile Wireless Home Agent provides these additional benefits:

- Supports static and dynamic IP address allocation.
- Attracts, intercepts, and tunnels datagrams for delivery to the MS.
- Receives tunneled datagrams from the MS (through the FA), unencapsulates them, and delivers them to the corresponding node (CN).

Note Depending on the configuration, reverse tunneling may, or may not, be used by the MS, and may or may not be accepted by the HA.

- Presents a unique routable address to the network.
- Supports ingress and egress filtering.
- Maintains binding information for each registered MS containing an association of Care-of Address (CoA) with the home address, NAI, and security keys together with the lifetime of that association.
- Receives and processes registration renewal requests within the bounds of the Mobile IP registration lifetime timer, either from the MS (through the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Receives and processes de-registration requests either from the MS (through the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Maintains a subscriber database that is stored locally or retrieved from an external source.
- Sends a binding update to the source PDSN under hand-off conditions when suitably configured.
- Supports dynamic HA assignment.

The Home Agent

The Home Agent (HA) maintains mobile user registrations and tunnels packets destined for the mobile to the PDSN/FA. It supports reverse tunneling, and can securely tunnel packets to the PDSN using IPSec. Broadcast packets are not tunneled. Additionally, the HA performs dynamic home address assignment for the mobile. Home address assignment can be from address pools configured locally, through either DHCP server access, or from the AAA server.

The Cisco HA supports proxy Mobile IP functionality, and is available on the Cisco 7600 series router, Cisco 7200 series router, and Cisco 6500 series switch platforms. A Cisco HA based on the Cisco 7200 series router supports up to 262,000 mobile bindings, can process 100 bindings per second, and is RFC 2002, RFC 2003, RFC 2005 and RFC2006 compliant.

A Cisco HA based on the Cisco 7600 series router or Cisco Catalyst 6500 switch, with two MWAM cards housing five active HA images and five standby images, would support the above figures multiplied by 5.

For more information on Mobile IP as it relates to Home Agent configuration tasks, please refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm.

CHAPTER 1

Planning to Configure the Home Agent

This chapter provides information that you should know before configuring a Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

- Supported Platforms, page 1-1
- Prerequisites, page 1-1
- Configuration Tasks, page 1-3
- Upgrading a Home Agent Image, page 1-3
- Required Base Configuration, page 1-7
- Configuration Examples, page 1-9
- Restrictions, page 1-13
- Supported Standards, MIBs, and RFCs, page 1-13
- Related Documents, page 1-14

Supported Platforms

The Cisco HA is available on Cisco's 7206VXR NPE-400 router, 7206VXR NPE-G1 router, 6500 series switch and 7600 series router. The HA supports Fast Ethernet and Gigabit Ethernet interfaces on these platforms.

Note Cisco Mobile Wireless Release 3.0, Cisco IOS Release 12.3(14)YX and later, supports both the standard MWAM 512 MB per processor memory option, and the 1 GB per processor memory option.

Prerequisites

Depending on the platform on which you are implementing a Home Agent, the prerequisites vary. The sections below provide general guidelines to follow before configuring a Cisco Mobile Wireless Home Agent in your network:

- Cisco 7200 Series Platform Prerequisites, page 1-2
- Catalyst 6500 / Cisco 7600 Series Platform Prerequisites, page 1-2

Cisco 7200 Series Platform Prerequisites

Ensure that you meet the following hardware and software requirements before you implement a Home Agent in your network on the Cisco 7200 series router platform.

Home Agent on the Cisco 7206VXR NPE-400

For platform details and complete list of interfaces supported on 7206VXR NPE-400, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_book09186a008007daa6.html

The supported configuration on a Cisco 7206VXR with NPE-400 processor is with 512MB DRAM and one PA-2FE-TX FE port adopter, or two PA-FE-TX port adaptors. PA-2FE-TX port adaptor has two 10/100 based Ethernet ports. PA-FE-TX port adapter has one 10/100 based Ethernet port. The I/O controller on the NPE-400 processor supports two more 10/100 based Ethernet ports. Because the PA-FE-TX is end-of-sale, new configurations require the PA-2FE-TX port adaptor.

For IPSec support, a service adaptor (SA-ISA or SA-VAM2) is required. Because SA-ISA is end-of-sale, new configurations utilizing IPSec will require the NPE-G1 with SA-VAM2.

Home Agent on 7206VXR NPE-G1

For platform details and complete list of interfaces supported on 7206VXR NPE-G1, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a0080201e63.html

The supported configuration on a Cisco 7206VXR NPE-G1 processor is with 1GB DRAM and one PA-2FE-TX FE port adaptor. The Cisco 7206VXR NPE-G1 has three 10/100/1000 based Ethernet Ports.

For IPSec support, a service adaptor SA-ISA or SA-VAM2 is required. Because the SA-ISA is end-of-sale, new configurations utilizing IPSec will require use of SA-VAM2

Catalyst 6500 / Cisco 7600 Series Platform Prerequisites

Home Agent on 6500 Series Switch

For platform details and a complete list of interfaces supported on the Cisco 6500 series switch, please refer to the on-line product information at the following url:
http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

The supported configuration for the HA based on the 6500 Series switch is dependent on the desired capacity, interface type to be deployed, and whether IPSec support is required.

Either a Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) and Policy Feature Card 2 (PFC2) is required, or a Supervisor Engine 720 with Multilayer Switch Feature Card 3 (MSFC3) and Policy Feature Card 3BXL (PFC3BXL) is required.

A 1GB MWAM or 512MB MWAM is required to run HA functionality. Each MWAM module supports up to 5 HA images (5 HA instances).

For IPSec support, an IPSec VPN Services Module (VPNSM) is required for each Cisco 6500 series switch chassis.

Home Agent on 7600 Series Router

For platform details and a complete list of interfaces supported on the Cisco 7600 series router, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

The supported configuration for the HA based on the Cisco 7600 Series switch is dependent on the desired capacity, interface type to be deployed, and whether IPSec support is required.

Either a Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) and Policy Feature Card 2 (PFC2) is required, or a Supervisor Engine 720 with Multilayer Switch Feature Card 3 (MSFC3) and Policy Feature Card 3BXL (PFC3BXL) is required.

A 1GB MWAM or 512MB MWAM module is required to run HA functionality. Each MWAM module supports 5 HA images (5 HA instances).

For IPSec support, an IPSec VPN Services Module (VPNSM) is required for each Cisco 7600 series switch chassis.

Configuration Tasks

The Cisco Home Agent software includes three images, one for the Cisco 7200 Series Router, one for the 7300 Series router, and one for the Cisco Catalyst 6500 switch and Cisco 7600 Series router platforms. This section describes the steps for configuring the Cisco Home Agent. Each image is described by platform number.

- c7200-h1is-mz HA image
- c7301-is-mz HA image
- svcmwam-h1is-mz HA image

Upgrading a Home Agent Image

To upgrade an image, you will need a compact flash card that has the MP partition from the current image or later, and a recent supervisor image. To locate the images, please go to the Software Center at Cisco.com (http://www.cisco.com/public/sw-center/).

To perform the upgrade perform the following procedure:

Step 1 Log onto the supervisor and boot the MP partition on the PC.

```
 router #hw-module module 3 reset cf:1
Device BOOT variable for reset = cf:1 Warning:  Device list is not verified.
 >
 > Proceed with reload of module? [confirm] % reset issued for module 3
 >router#
```

Step 2 Once the module is online, issue the following command:

copy tftp: *tftp file location* pclc# *linecard #*-fs:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
router #copy tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin pclc#3-fs:
  Destination filename [c6svcmwam-c6is-mz.bin]?
  Accessing tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin...
  Loading images/c6svcmwam-c6is-mz.bin from 10.102.16.25 (via Vlan1):
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  [OK - 29048727/58096640 bytes]

  29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
  router #

  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeeded>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module
```

Step 3 Boot the MWAM card back to partition 4, and you have an upgraded image.

```
router#hw-module module 3 reset
```

Upgrading the HA Image From XW-based Image to YX-based Image

If you are upgrading the Home Agent from a XW-based image to a 12.3(14)YX, or 12.4(11)T image, you first need to upgrade the SUP image from a SXB-based image to a SXE-based image.

Note We recommend that you upgrade to the Cisco IOS Supervisor Engine 720, Release 12.2(18)SXE3. For more information on the 12.2(18)SXE3 Supervisor image, please refer to the following URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

After you upgrade the SUP image, you can then upgrade the HA image.

Upgrading the Supervisor Image

To upgrade the Supervisor image, perform the following procedure:

Step 1 Copy the SUP image to the disks (disk0: / slavedisk0:).

Step 2 Add the following command to the running config **boot system disk0**: *SUP image name*". Here is an example:

```
boot system disk0:c6k222-pk9sv-mz.122-18.SXD2.bin
```

Note This step may require you to unconfigure previously configured instances of this CLI in order to enable the image to properly reload.

Step 3 Perform a "write memory" so that running configuration is saved on both active and standby SUP.

Step 4 Issue **reload** command on the active SUP.

Step 5 Both active and standby supervisors will reload simultaneously and come up with the SXD-based image.

Note Issuing the **reload command** on the active SUP will cause both the active and standby Supervisors to reload simultaneously, thus causing some downtime during the upgrade process.

Upgrading the HA Image on MWAM

To upgrade to the YF-based image on the MWAM, perform the following procedure:

Step 1 Bring down the active HA by issuing the **hw-module module** *slot #* **reset cf:1** command. The standby HA will take over as the active HA. Log onto the supervisor and boot the MP partition on the PC.

```
router #hw-module module 3 reset cf:1
Device BOOT variable for reset = cf:1 Warning: Device list is not verified.
>

> Proceed with reload of module? [confirm] % reset issued for module 3
>router#
```

Step 2 Once the module is online, copy the YF image to pclc# *slot* file system by issuing the following command:

copy tftp: *tftp file location* **pclc#** *linecard #***-fs**:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
router #copy tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin pclc#3-fs:
  Destination filename [c6svcmwam-c6is-mz.bin]?
  Accessing tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin...
  Loading images/c6svcmwam-c6is-mz.bin from 64.102.16.25 (via Vlan1):
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  [OK - 29048727/58096640 bytes]
  29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
  router #
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeeded>
  2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module
```

Step 3 Boot the MWAM card back to partition 4, and you have an upgraded image.

```
router#hw-module module 3 reset cf:4
```

Step 4 Verify that all the bindings opened with the active HA have synced with the processor with new image.

Step 5 Bring down the active HA with the XW-based image. The newly loaded YF-based HA will now become active.

Step 6 Perform steps 1 through 3 as described above.

Note The downgrade process is similar to the upgrade process; the SUP image should be downgraded first, followed by the HA image.

Note For SXD-based SUP images, if **config-on-SUP** mode is used on the MWAM, the startup configuration is written on both the SUP and local file system. This will assist you in upgrading or downgrading the images without losing the HA configuration between XW and YF images.

Note The downgraded image always starts with **config-local** due to incompatibility, and so it must be explicitly configured again using **config-on-sup** on every downgrade. Additionally, any further upgrades will start with the mode used by the same version the image used earlier, followed by the mode used by the old version.

Changing Configuration on Home Agent in a Live Network

If you need to change the working configuration on a Home Agent in a live network environment, perform the following procedure:

Step 1 Bring the standby HA out of service. An example would be to shut down the HSRP interface towards active HA.

Step 2 Make the necessary configuration changes on the standby HA, and save the configuration.

Step 3 Issue the **reload command to bring** the standby HA back into service.

Step 4 Bring the active HA out of service by shutting down HSRP interface. This will cause the standby to takeover as the active HA.

Step 5 Make the necessary configuration changes on the active HA, and save the configuration.

Step 6 Issue the **reload command to bring the active** HA back into service.

Note Some outage might occur concerning existing calls on the active HA being cleared forcibly.

Note For HA redundancy to work properly, configure the active and standby the same.

Loading the IOS Image to MWAM

The image download process automatically loads an IOS image onto the three processor complexes on the MWAM. All three complexes on the card run the same version of IOS, so they share the same image source. The software for MWAM bundles the images it needs in flash memory on the PC complex. For more information, refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note*.

Required Base Configuration

A typical HA configuration requires that you define interfaces in three directions: PDSN/FA, home network, and AAA server. If HA redundancy is required, then you must configure another interface for HSRP binding updates between HAs. If you are running the HA on the MWAM, the HA will see the access to one GE port that will connect to Catalyst 6500 backplane. That port can be configured as a trunk port with subinterfaces provided for each necessary network access.

VLANs can be defined corresponding to each interface: PDSN/FA, home network, AAA. In the case of multiple HA instances in the same Catalyst 6500 chassis, or 7600 chassis, the same VLAN can be used for all of them.

The following sections illustrate the required base configuration for the Cisco Mobile Wireless Home Agent:

- Basic IOS Configuration on MWAM, page 1-7
- Configuring AAA in the Home Agent Environment, page 1-8
- Configuring RADIUS in the Home Agent Environment, page 1-9
- Configuration Examples, page 1-9

Basic IOS Configuration on MWAM

To configure the Supervisor engine to recognize the MWAM modules, and to establish physical connections to the backplane, use the following commands:

	Command	Purpose
Step 1	`router# vlan database`	Enter VLAN configuration mode.
Step 2	`router(vlan)# vlan vlan-id`	Add an Ethernet VLAN.
Step 3	`router(vlan)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	`router(config)# mwam module 7 port 3 allowed-vlan vlan_range`	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM.
Step 5	`router# session slot MWAM module processor processor number`	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM. ***Processor number* is from 2 to 6**.
Step 6	`Router(config)# int gigabitEthernet 0/0`	Specifies the type of interface being configured, and the slot number.
Step 7	`Router(config-if)# no shut`	Puts the specified GE interfaces in service.

	Command	Purpose
Step 8	`Router(config-if)# int gigabitEthernet 0/0.401`	Specifies the type of interface being configured, and the slot number.
Step 9	`Router(config-subif)# encapsulation dot1Q 401`	Enables IEEE 802.1Q encapsulation of traffic on a specified sub interface in virtual LANs.
Step 10	`Router(config-subif)# ip address 10.1.1.1 255.255.255.0`	Specifies the IP address.
Step 11	`Router(config-subif)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.

Note MWAM modules synchronize their timing functions from the Supervisor engine's clock timers. Do not configure the timers on each individual MWAM.

Configuring AAA in the Home Agent Environment

Access control is the way you manage who is allowed access to the network server and what services they 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. For detailed information about AAA configuration options, refer to the "Configuring Authentication," and "Configuring Accounting" chapters in the *Cisco IOS Security Configuration Guide*.

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

	Command	Purpose
Step 1	`Router(config)# aaa authentication ppp default group radius`	Enables authentication of PPP users using RADIUS.
Step 1	`Router(config)# aaa authorization network default group radius`	Restricts network access to a user. Runs authorization for all network-related service requests. Uses the group radius authorization method as the default method for authorization.

Configuring RADIUS in the Home Agent Environment

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*.

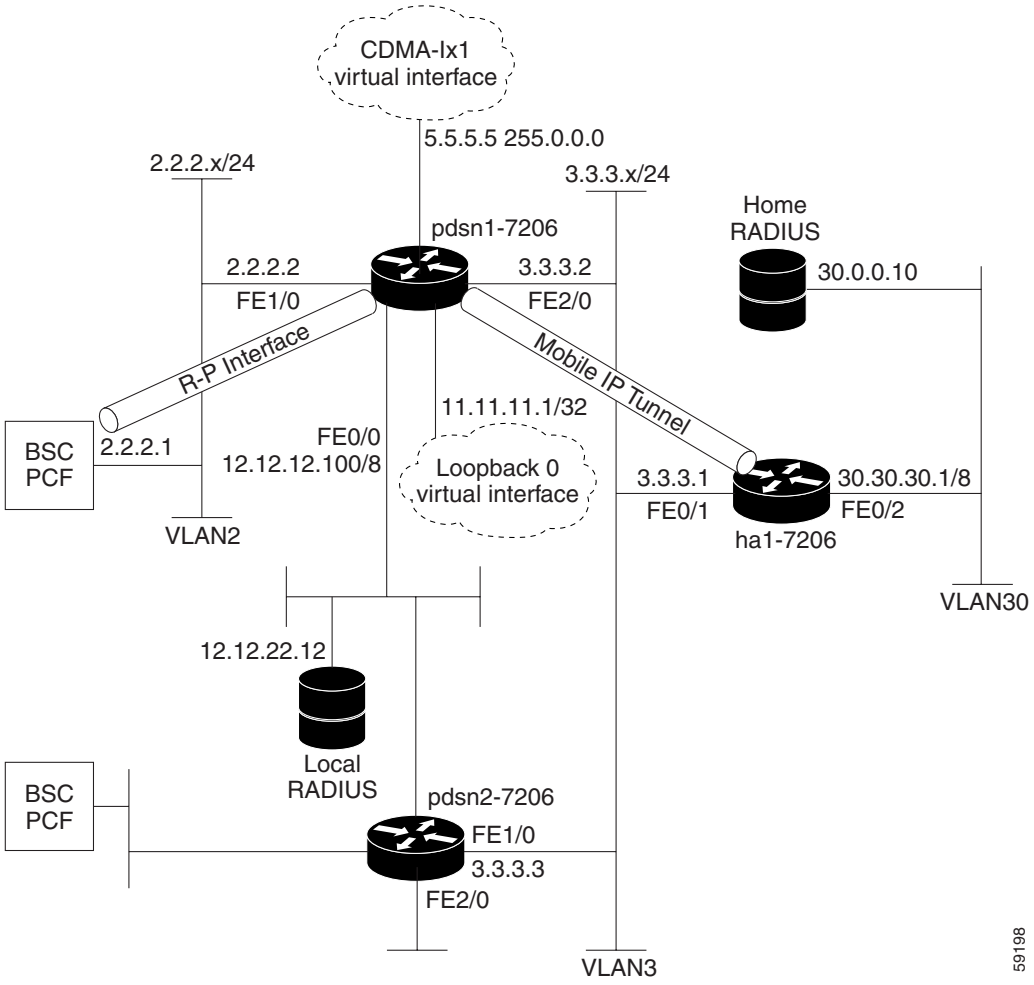
To configure RADIUS in the HA environment, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host ip-addr key sharedsecret`	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.

Configuration Examples

Figure 1-1 and the information that follows is an example of the placement of a Cisco HA and it's configuration.

Figure 1-1 Home Agent —A Network Map



Example 1

```
hostname ha1-7206
!
aaa new-model
!
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
interface FastEthernet0/1
 description To FA/PDSN
 ip address 3.3.3.1 255.255.255.0
!
interface FastEthernet0/2
 description To AAA
 ip address 10.30.30.1 255.0.0.0
!
router mobile
!
```

```
ip local pool ha-pool1 10.35.35.1 35.35.35.254
ip mobile home-agent broadcast
ip mobile virtual-network 10.35.35.0 255.255.255.0
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 10.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
line con 0
 exec-timeout 0 0
 login authentication CONSOLE
```

Example 1-1 Home Agent Configuration

```
Cisco_HA#sh run
Building configuration...

Current configuration : 4532 bytes
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname USER_HA
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa session-id common
!
username simulator password 0 cisco
username userc-moip password 0 cisco
username pdsn password 0 cisco
username userc password 0 cisco
username USER_PDSN
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
! !
!
 interface Loopback0
 ip address 10.2.2.2 255.255.255.0
!
interface Tunnel1
 no ip address
!
```

```
interface FastEthernet0/0
 ip address 10.15.68.14 255.255.0.0
 duplex half
 speed 100
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex half
 speed 10
 no cdp enable
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 ip address 10.5.5.3 255.255.255.0 secondary
 ip address 10.5.5.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.15.254
ip local pool ha-pool1 10.4.4.100 10.4.4.255
ip default-gateway 10.15.0.1
ip classless
ip route 10.3.3.1 255.255.255.255 FastEthernet1/1
ip route 10.100.0.1 255.255.255.255 9.15.0.1
ip route 10.17.17.17 255.255.255.255 FastEthernet1/0
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile host nai userc-moip address pool local ha-pool interface FastEthernet1/0
ip mobile host nai userc address pool local pdsn-pool interface Loopback0 aaa
ip mobile secure host nai userc-moip spi 100 key hex ffffffffffffffffffffffffffffffff
replay timestamp within 150
!
!
radius-server host 10.15.200.1 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!

gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
line vty 5 15
!
!
end
```

Restrictions

Simultaneous Bindings

The Cisco Home Agent does not support simultaneous bindings. When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required, because it is used to maintain more than one flow to the same IP address.

Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

Supported Standards, MIBs, and RFCs

RFCs

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following RFCs:

- IPv4 Mobility, RFC 2002
- IP Encapsulation within IP, RFC 2003
- Applicability Statement for IP Mobility Support, RFC 2005
- The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006
- Reverse Tunneling for Mobile IP, RFC 3024
- Mobile IPv4 Challenge/Response Extensions, RFC 3012
- Mobile NAI Extension, RFC 2794
- Generic Routing Encapsulation, RFC 1701
- GRE Key and Sequence Number Extensions, RFC 2890
- IP Mobility Support for IPv4, RFC 3220, Section 3.2 Authentication
- The Network Access Identifier, RFC 2486, January 1999.
- An Ethernet Address Resolution Protocol, RFC 826, November 1982
- The Internet Key Exchange (IKE), RFC 2409, November 1998.
- Cisco Hot Standby Routing Protocol (HSRP), RFC 2281, March 1998

Standards

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following standards:

- TIA/EIA/IS-835-B, TIA/EIA/IS-835-C and TIA/EIA/IS-835-D

MIBs

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following MIBs:

- CISCO- MOBILE-IP-MIB—provides enhanced management capabilities.
- Radius MIB—as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999.

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The HA supports the MIB defined in The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.

A full list of MIBs that are supported on the 7200, 7600 and 6500 series platforms can be found on Cisco web at the following URL:

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

Session counters maintained in the MIB cannot be reset using SNMP or CLI. The Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

The following additional counters will be supported in the Cisco Mobile Wireless Home Agent Release 3.0 MIB:

- Number of Bindings for FA/CoA
- Number of registration requests received per FA/CoA
- Failure counters per FA/CoA—HA Release 2.0 and above supports global failure counters. A per-FA/CoA counter will be added for each of those counters

Related Documents

Cisco IOS Software Documentation

- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.3
- *Cisco IOS Dial Technologies Command Reference*, Release 12.3
- *Cisco IOS Interface Configuration Guide*, Release 12.3
- *Cisco IOS Interface Command Reference*, Release 12.3
- *Cisco IOS IP Configuration Guide*, Release 12.3
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.3
- Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.3
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.3
- *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3
- *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3
- *Cisco IOS Security Configuration Guide*, Release 12.3

- *Cisco IOS Security Command Reference*, Release 12.3
- *Cisco IOS Switching Services Configuration Guide*, Release 12.3
- *Cisco IOS Switching Services Command Reference*, Release 12.3
- *Cisco Multi-Processor WAN Application Module Installation and Configuration Note*