Cisco 3200 Series Mobile Access Router Software Configuration Guide

October 14, 2004

Corporate 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: 408 526-4100

Customer Order Number: 85-4201-05=
Text Part Number: OL-1926-06

Cisco 3200 Series Mobile Access Router Software Configuration Guide

Preface

This document describes how to configure assembled Cisco 3200 Series Mobile Access Routers. For information regarding the specific hardware configuration of your router, contact your vendor.

Note The *Cisco 3200 Series Mobile Router Software Configuration Guide* was completed before the finished product was shipped. Therefore, that guide might not exactly represent the Cisco 3200 Series Mobile Access Router. However, any differences are subtle and should not affect overall use of the system or the performance of certain tasks. For the latest information, refer to **http:\www.cisco.com**.

Document Organization

This guide is organized as follows:

Chapter 1, "Introduction," provides an overview of the Cisco 3200 Series Mobile Access Routers and tells how the router fit into the larger network.

Chapter 2, "Cisco 3200 Series Mobile Access Router Interfaces," describes how the Cisco 3200 Series router interfaces can be accessed.

Chapter 3, "Introduction to Mobile IP," provides an overview of Mobile IP, as it relates to the Cisco 3200 Series router.

Chapter 4, "Basic Home Agent and Foreign Agent Configurations," describes how to enable mobile access router services on the router, a foreign agent, and a home agent.

Chapter 5, "Wireless LAN Example Scenario," provides an example of a Cisco 3200 Series router deployed in a public safety situation.

Chapter 6, "Static and Dynamic Network Configuration," describes static and dynamic router network configuration.

Chapter 7, "Static and Dynamic Collocated Care-of Address," describes how the router is allowed to roam to foreign networks where foreign agents are not deployed.

Chapter 8, "Foreign Agent Route Optimization," describes how the router *injects* mobile network routes into a foreign agent routing table, improving deployments that are running latency-sensitive applications.

Chapter 9, "Mobile IP Security," describes the registration messages and the Mobile-Home Authentication Extension (MHAE).

Chapter 10, "Zeroization," describes how the zeroization feature erases all potentially sensitive information in the router memory.

Chapter 11, "Redundancy in a Mobile Environment," describes Mobile IP redundancy and provides example configurations.

Chapter 12, "Quality of Service for Cisco 3200 Routers," provides a description of the QoS features, such as Class Based Weighted Fair Queuing (CBWFQ), Network Based Application Recognition (NBAR), and Class Based Packet Marking.

Chapter 13, "Modems in a Mobile Environment," describes the GPRS/CDMA modems that provide the mobile access router with a layer 2 roaming interface.

Chapter 14, "FESMIC Switch Port Functionality," provides an overview of VLANs, IGMP Snooping, and Auto-negotiation.

Chapter 15, "IEEE 802.1Q Configuration," describes how to configure IEEE 802.1Q Configuration for the Cisco 3200 Series router.

Chapter 16, "MIB Support," describes Mobile IP MIB support for the Simple Network Management Protocol (SNMP).

Chapter 17, "Configuring SNMP," provides an example of a Cisco 3200 Series router deployed in a public safety situation.

Chapter 18, "Troubleshooting the Cisco 3200 Series Mobile Access Router," provides some information on troubleshooting a Cisco 3200 Series router

Audience and Scope

The audience for this document is the system integrator (SI) and system engineer (SE). They are experts, with networking industry training and experience. We assume that users are familiar with the terminology and concepts of the PC-104, IOS, and Mobile IP networking.

The SI or SE uses this document to configure the router to communicate with peripheral devices through the network and to troubleshoot the cards. Although they might not be specifically identified as SIs or SEs, all users of this documentation are assumed to have comparable skills and knowledge.

Related Documentation

We recommend, "Fundamentals of Wireless LANs" (ISBN 1-58713-119-6) by Cisco Press.

You can access the followin documents on the Documentation page on Cisco Connection Online (CCO) at www.cisco.com.

- *Cisco 3200 Series Mobile Access Router Card Release Notes*
- *Cisco 3200 Wireless MIC Software Configuration Guide*
- *Cisco IOS Command Reference for Access Points and Bridges*
- *Cisco 3200 Series Mobile Access Router Hardware Reference*
- *Cisco IOS IP and IP Routing Command Reference*

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

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

For information about using Cisco IOS software to configure SNMP, refer to the following documents:

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

See also RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*.

Documentation Locations

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Cisco Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package. The Cisco Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page. You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Documentation Conventions

This guide uses the following conventions for information and instructions.

Notes, Cautions, and Warnings

Notes, cautions, and warnings use the following conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

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

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this IAD.**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij7 elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

Commands

Table 1 describes the syntax used with the commands in this document.

Table 1 Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{**x** | **x** | **x**}	A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Documentation CD

The *Cisco 3200 Series Router Documentation CD* contains the technical publications for the Cisco 3200 Series Mobile Access Router. To view the documentation requires Acrobat Reader 4.0 or higher.

Major topics are broken into PDF files and the file names are the same as the section names. Each PDF file contains a complete set of bookmarks, so you can jump to any topic in any file by double-clicking a bookmark.

After the CD is inserted in the CD ROM drive and recognized by your PC, do the following:

Step 1 Open Windows Explorer.

Step 2 Access the CD drive.

Step 3 Double click any PDF file.

A single file named EntireBook.PDF contains the entire book, as opposed to the file being broken into sections, primarily for the purpose of printing the entire book.

System Requirements

Processor	Pentium 150 MHz or faster recommended
PC Operating System	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows ME Microsoft Windows XP Microsoft Windows NT 4.0 Microsoft Windows 2000
Memory	64-MB DRAM
Drives	4x CD-ROM drive
Monitor	Color monitor capable of 800 x 600 pixel resolution
Software	Adobe Acrobat Reader 4.0 or later

Printing Documents

The documentation is organized into sections.

To print a document section:

Step 1 Click the **Printer** icon on the Acrobat toolbar.

The Windows Print Dialog box appears.

Step 2 Select your default printer, and click **OK**.

To print the entire book:

Step 1 Open Windows Explorer.

Step 2 Access the CD drive.

Step 3 Double click the EntireBook.PDF file.

Step 4 Click the **Printer** icon on the Acrobat toolbar.

The Windows Print Dialog box appears.

Step 5 Select your default printer, and click **OK**.

Sending CD Feedback

This CD was created with simplicity in mind. We hope that you find it easy to navigate and that it contains the information that you need to successfully install and configure your router. Please feel free to provide us with your feedback about the CD interface, the information on the CD, and the usefulness of the content.

To provide feedback directly to the Cisco 3200 Series Mobile Access Router documentation team, e-mail us at **doccd-feedback-smb@cisco.com**.

Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Introduction

The Cisco 3200 Series Mobile Access Routers deliver *always on* IP connectivity for networks in motion. These routers are intended to be mounted on a vehicle. They support Cisco IOS Mobile Networks, and allows them to *hide* the IP roaming from the local IP nodes. This allows IP hosts on a mobile network to connect transparently to the parent network while a router is in motion.

For example, an airplane equipped with Cisco 3200 Series Mobile Access Router can fly around the world while passengers stay connected to the Internet. The client computers do not need any specialized software to maintain the connections. This transparent communication is accomplished by Mobile IP devices that tunnel packets to the mobile access router.

The Cisco 3200 Series Mobile Access Router includes a third-party power source, cables, and an enclosure, that are assembled and installed by your system integrator. This document provides the information that you need to configure a completed Cisco 3200 Series Mobile Access Router.

Caveats

The following caveat applies to the Cisco 3200 Series Mobile Access Router.

Fast Ethernet Support

The FastEthernet 0/0 port on the MARC is a 10/100 Fast Ethernet *router* port. The FastEthernet 1/0 through 1/3 or 2/0 through 2/3 or 3/0 through 3/3 ports (as determined by the position of the rotary switch) on the 4-port FESMIC and the FastEthernet 1/0 and 1/1 or 2/0 and 2/1 or 3/0 and 3/1 ports on the 2-port FESMIC are 10/100 Fast Ethernet *switch* ports. The switch ports support all layer 2 features. The routing features supported on the MARC cannot be configured on the FESMIC ports.

Secure MAC Address

Network security is implemented by providing the user with option to make a port secure by allowing only well known MAC addresses to send in data traffic. Secure MAC addresses can be provisioned to allow forwarding of only secure addresses on a FESMIC 10/100 Fast Ethernet port.

IOS Switching Features that are Not Supported

The switching features described in this section are not supported on the Cisco 3200 Series router.

Fast Ether Channel

Fast Ether Channel (FEC), which allows multiple physical Fast Ethernet links to be combined into one logical channel.

SPAN

The Switched Port Analyzer (SPAN), sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

Voice VLAN

Voice VLAN allows a switch access port to receive an 802.1Q tagged voice packet and native data packet from IP phones with a local switch port that connects to data network. VLAN–capable IP phones are powered directly from the switch port. The FESMIC does not provide in–line power.

Hardware Flow Control

Flow control is not available on the 10/100 Fast Ethernet interfaces of the FESMIC.

CGMP

Cisco Group Management Protocol (CGMP) was implemented by Cisco to restrain multicast traffic in a Layer 2 network. CGMP is not supported due to the lack of common code support.

Sub-interface Support

The **sub-interface** command is not supported for the virtual layer 3 interface and layer 2 interface on the FESMIC.

Switch Virtual Interface (SVI) is a virtual interface, and Cisco Discovery Protocol (CDP) cannot be enabled on the SVI interface. The IP address can only be configured on the virtual layer 3 interface on the FESMIC.

The **class-map** command is used to define a traffic class. The **match cos traffic** command is not available for the SVI interface. Use the **mls qos map** global configuration command to define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map.

We recommend that you use a different VLAN identifier for the **interface vlan xx** and **vlan dot1q encap** commands when configuring the MARC 10/100 Fast Ethernet port.

Currently, the bridge-group functionality for the IP traffic on the SVI interface is not supported.

IOS Support

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out whether a feature is available in a given Cisco IOS software image, use Feature Navigator or the IOS Software Release Notes.

Feature Navigator

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

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at http://www.cisco.com/go/fn.

IOS Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables and descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release.

Mobile IOS Features

Table 1-1 compares mobile IOS features and stationary IOS features.

Table 1-1 Comparison of Mobile IOS Features and Stationary IOS Features

Feature	Stationary	Mobile
IP Addressing IPv4	X	X
IP Addressing IPv6	X	
IP Switching (Process, Cisco Express Forwarding (CEF), Fast)	X	X

Table 1-1 Comparison of Mobile IOS Features and Stationary IOS Features (continued)

Feature	Stationary	Mobile
IP Routing IPv4 (Routing Information Protocol (RIP) version 2, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP))	X	X
IP Routing IPv6 (RIPv2)	X	
Encapsulation on serial interface (High-Level Data Link Control (HDLC)), Point-to-Point Protocol (PPP), Frame Relay, X.25, X.25 over TCP (XOT)	X	X
Bridging (transparent, integrated routing and bridging)	X	
DHCP Client	X	
DHCP Relay	X	X
DHCP Server	X	X
Domain Name System (DNS) Proxy and Spoofing	X	
Network Address Translation (NAT) and Port Address Translation (PAT)	X	
Network Time Protocol (NTP) Client	X	X
Generic Routing Encapsulation (GRE) Tunneling	X	X
Stacker (STAC) data compression	X	X
IP Security	X	X
IP Multicast Protocol Independent Multicast (PIM) sparse mode	X	
quality of service (QoS), Resource Reservation Protocol (RSVP)	X	
quality of service (QoS), Weighted Random Early Detection (WRED), Committed Access Rate (CAR), Link Fragmentation and Interleaving (LFI), Low Latency Queuing (LLQ), Differentiated Services Code Point (DSCP), Class-based Weighted Fair Queueing (CBWFQ), Network Based Application Recognition (NBAR), Class Based Packet Marking, Class Based Policer for the DSCP, Class Based Ethernet COS Matching and Marking (802.1p COS), Priority Queueing (PQ), Traffic Policing, Class Based Policer for the DiffServ Assured Forwarding (AF) PHB, DiffServ Compliant WRED, Flow Based WRED, Random Early Detection (RED), LLQ for Frame Relay, Custom Queueing (CQ), and General Traffic Shaping (GTS)	X	X
Authentication (Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and MS-CHAP	X	X
Asynchronous Tunneling	X	X
CHAT Dialing Scripts, DDR	X	X
Cisco Firewall Phase I and Phase II	X	X
Cisco Secure Intrusion Detection	X	X
Service Assurance Agent	X	X
IP Named/Numbered Access-lists	X	X

Feature	Stationary	Mobile
Secure Shell Version 1	X	X
RADIUS and TACACS+	X	X
Simple Network Management Protocol (SNMP)	X	X
IPSEC VPN/ Internet Key Exchange (IKE) AES	X	X
Syslog	X	
Cisco Discovery Protocol (CDP)	X	
Packet Assembler/Disassembler (PAD)	X	

RFCs Supported

The following RFCs are supported:

- RFC 2002, *IP Mobility Support*
- RFC 2281, *Cisco Hot Standby Router Protocol*

Network Management Support (Cisco View)

CiscoView is a web-based, graphical device management application that provides monitoring and configuration features for Cisco internetworking products (switches, routers, hubs, concentrators, and access servers). CiscoView aides network management by displaying a physical view of a Cisco device, allowing users to easily interact with device components to change configuration parameters or monitor statistics.

Software Features

Table 1-2 Cisco 3200 Series Mobile Access Router Supported Software Features

Feature	Supported[1]	Image	Comments
AAA Server, RADIUS, TACACS			
AAA Broadcast Accounting	I	IP, IP+	Allows accounting information to be spanned to more than one authentication, authorization, and accounting (AAA) server server. AAA server subsystem is required for RADIUS and TACACS support.
AAA DNIS Map for Authorization	I	IP, IP+	Obsoleted by the AAA Server Groups based on Dialed Number Information Service (DNIS).
AAA Server Group	I	IP, IP+	Servers are grouped based on services configured on the AAA servers.

Table 1-2 Cisco 3200 Series Mobile Access Router Supported Software Features (continued)

Feature	Supported[1]	Image	Comments
AAA Server Group Dead Timer	I	IP, IP+	Allows each AAA server to be fully configured in server group. Only works with RADIUS.
AAA Server Group Enhancements	I	IP, IP+	Allows each AAA server to be fully configured in server group. Only works with RADIUS.
AAA Server Groups Based on DNIS	I	IP, IP+	Router can use the DNIS to select a particular AAA server group.
Message Banners for AAA Authentication	I	IP, IP+	Displays custom success and failure login message.
Named Method Lists for AAA Authorization and Accounting	I	IP, IP+	Defines the way authorization is performed and the sequence.
RADIUS	Yes	IP, IP+	
TACACS+	Yes	IP, IP+	
Additional Vendor-Proprietary RADIUS Attributes	I	IP, IP+	Adds vendor specific extensions. Part of the RADIUS subsystem.
Authentication Proxy Accounting for HTTP	No		Accounting records for billing and security auditing. Service provider image only.
QoS Features			
Generic Traffic Shaping (GTS)	Yes	IP, IP+	
Class Based Ethernet CoS Matching & Marking (ISL CoS)	Yes	IP, IP+	ISL encapsulation is not supported. Class-based Packet Marking supports all packet marking CoS features.
Class Based Ethernet CoS Matching & Marking (802.1p CoS)	Yes	IP, IP+	
Class Based Policer for the DiffServ AF PHB	Yes	IP, IP+	
Class Based Weighted Fair Queuing (CBWFQ)	Yes	IP, IP+	
Class-Based Packet Marking - Differentiated Services Codepoint (DSCP)	Yes	IP, IP+	
Class-Based Packet Marking – Setting IP Precedence bits	Yes	IP, IP+	
Class-Based Packet Marking – QoS Group Value	Yes	IP, IP+	Class-based Packet Marking supports all packet marking CoS features.

Table 1-2 Cisco 3200 Series Mobile Access Router Supported Software Features (continued)

Feature	Supported[1]	Image	Comments
Class-Based Policer for the DSCP	Yes	IP, IP+	
Class-Based Policer for the DiffServ Assured Forwarding (AF) PHB	Yes	IP, IP+	
Class-Based Ethernet COS Matching and Marking (802.1p COS)	Yes	IP, IP+	
Class-Based Packet Marking – ATM CLP	Yes	IP, IP+	Class-based Packet Marking supports all packet marking CoS features.
Custom Queueing (CQ)	Yes	IP, IP+	
Committed Access Rate (CAR)	Yes	IP+	
Diffserv Compliant WRED	Yes	IP, IP+	
Flow-Based WRED	Yes	IP, IP+	
General Traffic Shaping (GTS)	Yes	IP, IP+	
Low Latency Queueing (LLQ)	Yes	IP, IP+	
Low Latency Queueing (LLQ) for Frame Relay	Yes	IP, IP+	
Network Based Application Recognition (NBAR)	Yes	IP+	
Priority Queueing (PQ)	Yes	IP, IP+	
QoS Packet Marking	Yes	IP, IP+	Same as Class-Based Marking (DSCP, IP precedence).
QoS Policy Propagation by using Border Gateway Protocol (QPPB)	Yes	IP, IP+	
Random Early Detection (RED)	Yes	IP, IP+	
RSVP support for LLQ	No	IP, IP+	
RSVP support for Frame Relay	No	IP, IP+	Part of the Frame Relay Traffic shaping subsystem.
Traffic Policing	Yes	IP+	
Weighted Fair Queueing (WFQ)	Yes	IP, IP+	
Weighted RED (WRED)	Yes	IP, IP+	
LFI	Yes	IP, IP+	

Table 1-2 Cisco 3200 Series Mobile Access Router Supported Software Features (continued)

Feature	Supported[1]	Image	Comments
RSVP	No	IP+	
COPS for RSVP	I	IP, IP+	RSVP subsystem has dependencies on COPS.
PPP and Related Protocols			
PPP	Yes	IP, IP+	
Multilink PPP	Yes	IP, IP+	
PPP Over Fast Ethernet 802.1Q	No	IP, IP+	Part of the VPN subsystem.
PPP over Frame Relay	Yes	IP, IP+	
PPPoE on Ethernet	I	IP, IP+	Part of the VPN subsystem
Compression Control Protocol	SB	IP, IP+	
Challenge Handshake Authentication Protocol (CHAP)	Yes	IP, IP+	
Bandwidth Allocation Control Protocol (BACP)	SB	IP, IP+	
MS Callback	I	IP, IP+	Part of Dialer subsystem.
MS-CHAP Support	Yes	IP, IP+	
Password Authentication Protocol (PAP)	Yes	IP, IP+	
Double Authentication	No	IP, IP+	This feature is on the NAS or Network Access Server side to work with a AAA server to authenticate a remote user in addition to CHAP/PAP authentication on the PPP session. This does not seem applicable to Hercules-A.
Easy IP, DHCP, Auto Install			
Easy IP (Phase 1)	Yes	IP, IP+	
DHCP Client	Yes	IP, IP+	
DHCP Proxy Client	I		Part of DHCP client subsystem
DHCP relay	Yes	IP, IP+	
DHCP Relay Agent Support for Unnumbered Interfaces	Yes	IP, IP+	The Cisco IOS DHCP Relay Agent Support for Unnumbered Interfaces reduces configuration tasks and costs. Whenever an unnumbered interface is configured, a static route for any host beyond the unnumbered interface must be manually configured. For DHCP relay, this static route is automatically maintained.

Table 1-2 Cisco 3200 Series Mobile Access Router Supported Software Features (continued)

Feature	Supported[1]	Image	Comments
DHCP Server	Yes	IP, IP+	
Import and Auto Configuration	Yes	IP, IP+	
Easy IP Phase 2	Yes	IP, IP+	
Auto Install Using DHCP for LAN Interfaces	Yes	IP, IP+	
HTTP Security	Yes	IP, IP+	
NAT			
NAT-Support for NetMeeting Directory [Internet Locator Service (ILS)]	Yes	IP, IP+	
Dialer			
Dial backup	Yes	IP, IP+	
Dial on Demand Authentication Enhancements	No	IP, IP+	Large scale dial out eliminates the need to configure dialer maps on every network access server for every destination. Instead, you can create remote site profiles that contain outgoing call attributes (telephone number, service type, and so forth) on the AAA server. The profile is downloaded by the network access server (NAS) when packet traffic requires a call to be placed to a remote site.
Dial Peer Enhancements	No	IP, IP+	
Dial-on-demand	Yes	IP, IP+	
Dialer Idle Timer Inbound Traffic Configuration	Yes	IP, IP+	
Dialer profiles	Yes	IP, IP+	
Dialer Watch	No	IP, IP+	HSRP functionality on the dial area is needed for the disaster recovery. The current implementation of HSRP has limited advantage in the dial world. The backup router and backup links are not immediately available if the primary routers and links go down.
Firewall			
Firewall Feature Set	Yes	IP+	
Firewall Intrusion Detection System	Yes	IP+	

Feature	Supported[1]	Image	Comments
Context-Based Access Control (CBAC)	Yes	IP+	
Port to Application Mapping (PAM)	Yes	IP+	
Frame Relay			
Frame Relay	Yes	IP, IP+	
Frame Relay ELMI Address Registration	I	IP, IP+	Enables automated exchange of Frame Relay QoS parameter information between the Cisco router and the Cisco switch.
Frame Relay Encapsulation	Yes	IP, IP+	
Frame Relay End-to-End Keepalive	Yes	IP, IP+	
Frame Relay Fragmentation (FRF.12)	Yes	IP, IP+	
Frame Relay Fragmentation with Hardware Compression	No	IP, IP+	
Frame Relay FRF.9 Payload Compression	I	IP, IP+	A stream-oriented, multi-vendor-compatible compression scheme.
Frame Relay IP RTP Priority	No	IP, IP+	The Frame Relay IP RTP Priority feature provides a strict priority queueing scheme on a Frame Relay permanent virtual circuits (PVCs) for delay-sensitive data, such as voice. Voice traffic can be identified by the Real-Time Transport Protocol (RTP) port numbers and classified into a priority queue configured by the **frame-relay ip rtp priority** command. As a result, voice is serviced as strict priority in preference to other nonvoice traffic.
Frame Relay PVC Interface Priority Queueing	I	IP, IP+	Provides an interface-level priority queueing scheme where prioritization is based on destination PVC rather than packet contents. For example, Frame Relay PIPQ allows you to configure a PVC transporting voice traffic to have priority over a PVC transporting signalling traffic, and a PVC transporting signalling traffic to have priority over a PVC transporting data.
Frame Relay Router ForeSight	No	IP, IP+	Extends the Stratacom ForeSight traffic management to the router and allows end-to-end ForeSight traffic management on service provider and enterprise frame relay networks.

Feature	Supported[1]	Image	Comments
Frame Relay Switching Diagnostics and Troubleshooting	Yes	IP, IP+	
Frame Relay Traffic Shaping (FRTS)	Yes	IP, IP+	
Frame Relay Rate Enforcement	SB	IP, IP+	
Frame Relay Priority/Custom Queueing	SB	IP, IP+	
Frame Relay TCP header compression	SB	IP, IP+	
Frame Relay Inverse-ARP	SB	IP, IP+	
Frame Relay Switching	SB	IP, IP+	
Frame Relay LMI	SB	IP, IP+	
Frame Relay Tunneling	SB	IP, IP+	
Frame Relay with IPv6	SB	IP+	
IP and Other Routing Protocols			
IPv4	Yes	IP, IP+	
IPv6	Yes	IP+	
IP Named Access Control List	Yes	IP, IP+	
IP RTP Priority	I	IP, IP+	
IP Summary Address for RIPv2	Yes	IP, IP+	

Feature	Supported[1]	Image	Comments
IP Precedence for GRE Tunnels	Yes	IP, IP+	Copies the Type of Service (TOS) bits to the tunnel header and is used in Mobile IP tunnels. Even with static nodes, with the advent of virtual private network (VPN) and QoS applications, it is also desirable to copy the TOS bits when the router encapsulates the packets using GRE. Routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED). Prior to this feature, at generic route encapsulation-based tunnel endpoints the TOS bits (including the precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero.
Next Hop Resolution Protocol	I	IP, IP+	Routers, access servers, and hosts can use Next Hop Resolution Protocol (NHRP) to discover the addresses of other routers and hosts connected to a non-broadcast, multi-access (NBMA) network. With NHRP, systems attached to an NBMA network dynamically learn the NBMA address of the other systems that are part of that network, allowing these systems to directly communicate without requiring traffic to use an intermediate hop.
Cisco Discovery Protocol (CDP)	Yes	IP, IP+	
On Demand Routing (ODR)	SB	IP, IP+	On-Demand Routing (ODR) uses Cisco Discovery Protocol (CDP) to propagate the IP prefix.
OSPF	Yes	IP, IP+	
OSPF Flooding Reduction	SB **(M)**	IP, IP+	Reduces unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are flooded with the higher bit set, thus making them Do Not Age (DNA) LSAs.
OSPF Not-So-Stubby Areas (NSSA)	Yes	IP, IP+	
OSPF On Demand Circuit (RFC 1793)	I		
OSPF Packet Pacing	Yes	IP, IP+	Allows OSPF update packets paced automatically by 33 milliseconds to avoid update packets lost.

Feature	Supported[1]	Image	Comments
RIP	Yes	IP, IP+	
Triggered RIP	I	IP, IP+	
Enhanced IGRP (EIGRP)	Yes	IP, IP+	
Enhanced IGRP Stub Routing	Yes	IP, IP+	
Express RTP and TCP Header Compression	SB	IP, IP+	
Fast-Switched Compressed RTP	SB	IP, IP+	
Fast-Switched Policy Routing	SB	IP, IP+	
Fast-Switched SRTLB	No	IP, IP+	
Snapshot routing	SB	IP, IP+	A single router interface can call other routers during periods when the line protocol for the interface is up (active periods). The router dials to all configured locations during such active periods to get routes from all remote locations.
Generic Routing Encapsulation (GRE)	Yes	IP, IP+	
Hot Standby Router Protocol (HSRP)	SB	IP, IP+	
HSRP support for ICMP redirects	SB	IP, IP+	
Integrated Routing and Bridging (IRB)	Yes	IP, IP+	
Subnetwork Bandwidth Manager (SBM)	I	IP, IP+	Part of RSVP subsystem.
Internet Protocol Control Protocol (IPCP) address negotiation	Yes	IP, IP+	Part of Easy-IP functionality.
Policy-Based Routing (PBR)	Yes	IP, IP+	
RTP Header Compression	Yes	IP, IP+	
STAC Compression	Yes	IP, IP+	
Source-Route Bridging (SRB)	No	IP, IP+	
Transparent Bridging	Yes	IP, IP+	
BGP	Yes	IP, IP+	
BGP 4	Yes	IP, IP+	

Feature	Supported[1]	Image	Comments
BGP 4 Multipath Support	Yes	IP, IP+	
BGP 4 Prefix Filter and In-bound Route Maps	Yes	IP, IP+	
BGP 4 Soft Config	Yes	IP, IP+	
BGP Soft Reset	Yes	IP, IP+	
UDLR Tunnel ARP and IGMP Proxy	Yes	IP, IP+	Supports Mobile IP on asymmetric links. Part of the Tunnel subsystem.
Uni-Directional Link Routing (UDLR)	Yes	IP, IP+	Supports Mobile IP on asymmetric links.
IP CEF			
CEF Support for IP Routing between IEEE 802.1Q vLANs	Yes	IP, IP+	
CEF Switching for Routed Bridge Encapsulation	I	IP, IP+	Part of IPFIB subsystem.
CEF/dCEF - Cisco Express Forwarding	Yes	IP, IP+	
Virtual Profile CEF Switched	I	IP, IP+	
Virtual Profiles	I	IP, IP+	
Virtual Interface Template Service	I	IP, IP+	
VLANS & Layer2 Protocols			
Spanning Tree Protocol (STP)	Yes	IP, IP+	
Spanning Tree Protocol (STP) Extension	No	IP, IP+	Broadens the STP implementation with increased port identification capability, improved path cost determination, and support for a new VLAN bridge STP.
Turbo Flooding of UDP Datagrams	No	IP, IP+	Speeds up flooding of UDP datagrams using spanning-tree algorithm
IEEE 802.1Q VLAN Support	Yes	IP, IP+	
Layer 2 Forwarding-Fast Switching	No	IP, IP+	For NAS servers and part of the VPN subsystem.
IP Multicast			
PIM Version 1	Yes	IP, IP+	
PIM Version 2	Yes	IP, IP+	
Multicast BGP (MBGP)	No	IP, IP+	

Feature	Supported[1]	Image	Comments
Multicast NAT	SB	IP, IP+	
Multicast Routing Monitor (MRM)	I	IP, IP+	Part of IP Multicast subsystem.
Multicast Source Discovery Protocol (MSDP)	No	IP, IP+	Requires BGP configured.
IGMP Version 1	Yes	IP, IP+	
IGMP Version 2	Yes	IP, IP+	
IGMP Version 3	I	IP, IP+	Part of IP Multicast subsystem
IP Multicast Load Splitting across Equal-Cost Paths	I	IP, IP+	IP multicast load splitting is accomplished indirectly by consolidating the available bandwidth of all the physical links into a single tunnel interface. The underlying physical connections use existing unicast load-splitting mechanisms for the tunnel (multicast) traffic. Part of IP Multicast subsystem.
Source Specific Multicast (SSM)	I	IP, IP+	Part of IP Multicast subsystem
Source Specific Multicast (SSM) - IGMPv3, IGMP v3lite, and URD	I	IP, IP+	Part of IP Multicast subsystem.
Stub IP Multicast Routing	I	IP, IP+	Supports dense mode only. Part of IP Multicast subsystem.
Bidirectional PIM	I	IP, IP+	Part of IP Multicast subsystem.
CGMP	SB	IP, IP+	
VPN			
Virtual Private Dial-up Network (VPDN)	Yes	IP, IP+	.
VPN Tunnel Management	Yes	IP, IP+	
L2TP Dial-Out	Yes	IP, IP+	
L2TP Layer 2 Tunneling Protocol	Yes	IP, IP+	
L2TP Tunnel Preservation of IP TOS	Yes	IP, IP+	
IPSec			
IP Sec Network Security	Yes	IP+	
IP Sec Triple DES Encryption (3DES)	Yes	IP+	

Feature	Supported[1]	Image	Comments
IPSEC VPN/ Internet Key Exchange (IKE) AES	Yes	IP+	
IKE Extended Authentication (Xauth)	Yes	IP+	
IKE Mode Configuration	Yes	IP+	
IKE Security Protocol	Yes	IP+	
IKE Shared Secret Using AAA Server	Yes	IP+	
Certification Authority Interoperability (CA)	Yes	IP+	
Wildcard Pre-Shared Key	Yes	IP+	
Dynamic Crypto Map	Yes	IP+	
Tunnel Endpoint Discovery	Yes	IP+	
Manual Security Association	Yes	IP+	
Secure Shell Version 1			
Secure Shell SSH Version 1 Integrated Client	Yes	IP+	
Secure Shell SSH Version 1 Server Support	Yes	IP+	
Mobile IP			
Mobile IP	Yes	IP, IP+	
Mobile Networks	Yes	IP, IP+	
Home Agent/Mobile Router Redundancy	Yes	IP, IP+	
Mobile Router Preferred Interfaces	Yes	IP, IP+	
Mobile Router Reverse Tunneling	Yes	IP, IP+	
Mobile Router Asymmetric Links	Yes	IP, IP+	
Mobile Router Static and Dynamic Networks	Yes	IP, IP+	
Static CCOA	Yes	IP, IP+	
Dynamic CCOA	Yes	IP, IP+	Only through IPCP; DHCP is not supported.
Priority HA Assignment (Dynamic HA)	Yes	IP, IP+	

Feature	Supported[1]	Image	Comments
AAA Server and Mobile IP	Yes	IP, IP+	
X.25			
X.25	Yes	IP, IP+	
X.25 Closed User Group	Yes	IP, IP+	
X.25 Failover	Yes	IP, IP+	
X.25 Load Balancing	Yes	IP, IP+	
X.25 over Frame Relay (Annex G)	Yes	IP, IP+	
X.25 over TCP (XOT)	Yes	IP, IP+	
X.25 Remote Failure Detection	Yes	IP, IP+	
X.25 Switch Local Acknowledgement	Yes	IP, IP+	
X.28 Emulation	Yes	IP, IP+	
PAD Subaddressing	Yes	IP, IP+	
Protocol Translation (PT)	No	IP, IP+	
Virtual Templates for Protocol Translation	No	IP, IP+	
CUG Selection Facility Suppress Option	Yes	IP, IP+	
DNS based X.25 routing	SB	IP, IP+	
X.25 address insertion	SB	IP, IP+	
X.25 to X.121 address / PVC mapping	SB	IP, IP+	
X.25 switch function (routing/pvc)	Yes	IP, IP+	
SA Agent			
Service Assurance (SA) Agent	Yes	IP, IP+	
Service Assurance (SA) Agent Enhancements	No	IP, IP+	Provides tools for measuring network performance using FTP, which is one of the most popular traffic types in Internet service provider (ISP) networks, and jitter (one-way delay), which is important for applications such as Voice over IP (VoIP).

Feature	Supported[1]	Image	Comments
RMON Events and Alarms	SB	IP, IP+	A standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. RMON MIB agent can be used in conjunction with SNMP to monitor traffic using alarms and events.
Response Time Reporter (RTR)	Yes	IP, IP+	
Response Time Reporter (RTR) enhancements	Yes	IP, IP+	
SNMP			
SNMP	Yes	IP, IP+	
SNMP Support for IOS vLAN Subinterfaces	Yes	IP, IP+	
SNMP Version 3	Yes	IP, IP+	
SNMPv2C	Yes	IP, IP+	
Interface Index Persistence	Yes	IP, IP+	Allows interfaces to be identified with unique values which remain constant even when a device is rebooted.
Miscellaneous Features			
Asynchronous Rotary Line Queuing	No	IP, IP+	For demand circuit only. It depends on the rotary-group.
Network Time Protocol (NTP)	Yes	IP, IP+	
Lock-and-Key	Yes	IP, IP+	
Reflexive Access Lists	I		Part of the core IP subsystem.
Standard IP Access List Logging	Yes	IP, IP+	
Time-Based Access Lists	I	IP, IP+	Part of the core IP subsystem.
Time-Based Access Lists Using Time Ranges	I	IP, IP+	Part of the core IP subsystem.
Automatic modem configuration	I	IP, IP+	Part of the modemcap subsystem. Required for AUX port modem support.
CLI String Search	Yes	IP, IP+	

Feature	Supported[1]	Image	Comments
Commented IP Access List Entries	Yes	IP, IP+	Allows remarks to be included in any IP access list. The remarks make the access list easier for the network administrator to understand.
Line Printer Daemon (LPD)	No	IP+	
Parse Bookmarks	SB	IP, IP+	Parser optimization feature.
Parser Cache	Yes	IP, IP+	Optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines.
Per-User Configuration	No	IP, IP+	Provides a flexible, scalable and easily maintained solution for customers with a large number of dial-in users, such as CiscoSecure TACACS user entry.
Selective Virtual-Access Interface Creation	No	IP, IP+	
Manual Certificate Enrollment	Yes	IP+	Generates a certificate request, and accepts Certificate Authority (CA) certificates and the routers certificate using TFTP server or manual cut-and-paste operations.

1. Yes: Included in Image and tested.
   No: Not included in Image
   SB: Included in image, but may not be tested.
   I: Included in the image due to features dependent on these subsystems.

Cisco 3200 Series Mobile Access Router Interfaces

The Cisco 3200 Series routers can be configured through the console ports.

The following topics are described:

- Terminal Configuration
- Command Line Interface Basics
- Basic Mobile Access Router Interface Configuration
- Remote Access to the Router

The physical characteristics of the router console interface are described in the Cisco 3200 Series Mobile Access Router Hardware Reference.

For descriptions of configuration commands and the configuration options available, refer to the appropriate software publications listed in the "Related Documentation" section.

Timesaver

Before you begin, disconnect all WAN cables from the router to keep it from trying to run the AutoInstall process. The router tries to run AutoInstall whenever you power it on, if there is a WAN connection on both ends and the router does not have a valid configuration file stored in nonvolatile random-access memory (NVRAM) (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote Transmission Control Protocol/Internet Protocol (TCP/IP) host.

Terminal Configuration

To configure the router by using a terminal, make sure you configure the terminal to match the router console port as follows:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit

Command Line Interface Basics

The command–line interface (CLI) can be used to set the parameters for the Cisco IOS software loaded on the router. Because the CLI is divided into different modes, the commands available to you at any given time depends on which mode you are in. Each mode is indicated by the prompt. Entering a question mark (**?**) at the CLI prompt displays a list of available commands.

Command-Line Modes

When you log in to the CLI, you are in *User EXEC* mode. User EXEC mode allows monitoring of the router, but few of the commands available in this mode allow modification of the configuration. To modify the configuration, you must enter *Privileged EXEC* or *Enable* mode. From Privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can change to *global configuration* mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

Configuration modes allow you to make changes to the running configuration; the parameters that govern the behavior of the router. If you save the *running configuration* to the *startup configuration*, the command parameters are stored in a file in the router memory and executed when the router is powered on or rebooted.

If the router cannot successfully load an Cisco IOS, it displays ROM monitor (ROMMON) mode. A user can also choose to enter ROMMON mode. ROM monitor is described in the "Access ROM Monitor Mode" section in the"Troubleshooting the Cisco 3200 Series Mobile Access Router" chapter.

Table 2-1 describes how to enter and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Entering and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command, or press **Ctrl-Z**.
Interface configuration	From global configuration mode, specify an interface, using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command, or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

You have to enter only enough characters for the Cisco IOS to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
Router# show conf
```

Command-Line Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

Command	Purpose
help	Provides a brief description of the help system in any command mode.
abbreviated-command-entry<**?**>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Finding Command Options

The command syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space.

The Cisco IOS software displays a list and brief description of keywords and arguments available for a command. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip**

routing command; to enable IP routing after it has been disabled manually, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

command **|** {**begin | include | exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
Router# show interface | include protocol

FastEthernet1/0 is up, line protocol is up
Serial1/0 is up, line protocol is up
Serial1/1 is up, line protocol is up
Serial1/2 is administratively down, line protocol is down
Serial1/3 is administratively down, line protocol is down
```

For more information on the search and filter functionality, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Table 2-2 lists some error messages that you might encounter while using the CLI.

Common CLI Error Messages

		How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for the device to recognize the command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% 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 possible keywords that you can enter with the command are displayed.

Command History Buffer

The Cisco IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs.

By default, the router records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the Cisco IOS records during the current terminal session:

```
BR# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the Cisco IOS records for all sessions on a particular line:

```
BR(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

To recall commands from the history buffer, perform one of the actions listed in Table 2-3:

	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the **terminal history** global configuration command and **history** line configuration command.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Router# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Router(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Router(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 2-4 shows the keystrokes that you need to edit command lines.

Table 2-4 Editing Commands Through Keystrokes

	Keystroke[1]	Purpose
Move around the command line to make changes or corrections.	**Ctrl-B** or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The Cisco IOS provides a buffer with the last ten items that you deleted.	**Ctrl-Y**	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	

Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
BR(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
BR(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
BR(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
BR(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
BR(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the "Editing Commands Through Keystrokes" section on page 2-7.

Configuring a host name allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

`Router>` **`enable`** `Password:` *`password`* `Router#`	Enter enable mode. Enter the password. (The password prompt displays only if a password is configured.) You have entered enable or privileged EXEC mode when the prompt changes to `Router#`.
`Router#` **`configure terminal`** `Enter configuration commands, one per line. End with CNTL/Z.` `Router(config)#`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.
`Router(config)#` **`hostname`** *`router`* `Router(config)#`	Change the name of the router to a meaningful name. Substitute your host name for *`router`*.

`Router(config)# enable secret guessme`	Enter an enable secret password. This password limits access to the privileged EXEC mode. When a user types **enable** at the EXEC prompt (Router>) and an enable secret password is configured, they must enter the enable secret password to gain access to configuration mode. Substitute your enable secret for *guessme*.
`Router(config)# line con 0`	Enter line configuration mode to configure the console port. When you enter.line configuration mode.
`Router(config-line)# exec-timeout 0 0`	Prevent the router's EXEC facility from timing out if you do not type any information on the console screen for an extended period.
`Router(config-line)# exit` `Router(config)#`	Exit back to global configuration mode.

To verify that you configured the host name and password:

Enter the **show config** command:

```
Router# show config
Using 1888 out of 126968 bytes
!
version XX.X
.
!
hostname Router
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
```

Check the host name and encrypted password displayed near the top of the command output.

Exit global configuration mode and attempt to re-enter it using the new enable password:

```
Router# exit
.
Router con0 is now available
Press RETURN to get started.
Router> enable
Password: guessme
Router#
```

If you are having trouble, check the following:

Caps Lock is off.

You entered the correct passwords. Passwords are case sensitive.

To enable mobile access router services on the Cisco 3200 Series router, use the following commands beginning in global configuration mode:

`Router(config)# router mobile`	Enables Mobile IP on the router.
`Router(config)# ip mobile router`	Enables the mobile access router and enters mobile access router configuration mode.
`Router(mobile-router)# address ipaddress mask`	Sets the home IP address and network mask of the mobile access router.
`Router(mobile-router)# home-agent ip-address`	Specifies the home agent that the mobile access router uses during registration.
`Router(mobile-router)# register {extend expire seconds retry number interval seconds | lifetime seconds | retransmit initial milliseconds maximum milliseconds retry number}`	(Optional) Controls the registration parameters of the mobile access router.
`Router(mobile-router)# reverse-tunnel`	(Optional) Enables the reverse tunnel function.
`Router(mobile-router)# exit`	Exits mobile access router configuration mode.
`Router(config)# ip mobile secure home-agent address {inbound-spi spi-in outbound-spi spi-out | spi spi} key hex string`	Sets up home agent security associations. The address is the home IP address of the home agent.
`Router(config)# interface type number`	Enters interface configuration mode for the interface specified.
`Router(config-ip)# ip address ip-address mask`	Sets an IP address for the interface.
`Router(config-if)# ip mobile router-service {hold-down seconds | roam [priority value] | solicit [interval seconds] [retransmit initial min maximum seconds retry number]}`	Enables mobile access router services, such as roaming, on an interface.

Display the WMIC MAC Address

In Enable mode, you can display the MAC address by issuing a **show interface dot11Radio 0** command. For example:

```
wmic-uut#sh int dot11Radio 0
Dot11Radio0 is up, line protocol is up
  Hardware is 802.11G Radio, address is 0005.9a3e.a91a (bia 0005.9a3e.a91a)
  MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

The MAC address is displayed as the **Hardware is 802.11G Radio** parameter.

The MAC address is also displayed when the reload command is issued. For example:

```
Router#reload

System configuration has been modified. Save? [yes/no]: yes
Proceed with reload? [confirm]
Radio system: delayed or multiple reload request, ignored
```

```
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:02:31.770: %SYS-5-RELOAD: Reload requested by console.Xmodem
file system is available.
flashfs[0]: 136 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 8169984
flashfs[0]: Bytes available: 7828992
flashfs[0]: flashfs fsck took 34 seconds.
Base ethernet MAC Address: 00:05:9a:3d:32:01
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
```

The MAC address is displayed as the **Base ethernet MAC Address** parameter.

To verify the mobile access router configuration, use any of the following commands in EXEC mode:

Router# **show ip mobile globals**	Displays global information for mobile agents.
Router# **show ip mobile mobile-networks** [*address*]	Displays a list of mobile networks associated with the mobile access router.
Router# **show ip mobile host** [*address*]	Displays mobile node information.
Router# **show ip mobile secure host** [*address*]	Displays the mobility security associations for the mobile host.
Router# **show ip mobile interface**	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
Router# **show ip mobile router**	Displays configuration information and monitoring statistics for the mobile access router.
Router# **show ip mobile router traffic**	Displays the counters that the mobile access router maintains.
Router# **show ip route mobile**	Displays information about the agents for the mobile access router.
Router# **show ip mobile router interface**	Displays information about the interface that the mobile access router is using for roaming.
Router# **show ip mobile router registration**	Displays the pending and accepted registrations of the mobile access router and clear the counters.
Router# **debug ip mobile router** [**detail**]	Displays debug messages for the mobile access router.

Use the **copy system:running-config nvram:startup-config** command to save your running configuration to the startup configuration. The startup configuration contains all the parameters under which the router is operating. However, the startup configuration is in DRAM. If the router reloads the software or a power outage occurs, the running configuration is erased.

The startup configuration is stored in NVRAM. When the router is reloaded or powered on, the startup configuration file is copied to the running configuration file. By saving the changes to the startup configuration, your configuration parameters will not be lost.

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

To prevent the loss of the router configuration, save it to NVRAM.

	Command	Purpose
Step 1	`Router>` **`enable`** `Password:` *`password`* `Router#`	Enters enable mode. Enter the password. You have entered enable mode when the prompt changes to `Router#`.
Step 2	`Router#` **`copy running-config startup-config`**	Copies the running configuration file to the startup configuration file in NVRAM.
Step 3	`Router(config-if)#` **`Ctrl-z`** `Router#` `%SYS-5-CONFIG_I: Configured from console by console`	Returns to enable mode. This message is normal and does not indicate an error.

Basic Mobile Access Router Interface Configuration

This section describes how the mobile access router ports can be accessed through the CLI. The physical characteristics of the Cisco 3200 Series router interfaces are described in the "Cisco 3200 Series Router Hardware Reference."

Fast Ethernet Interface Configuration

This section describes the basic configuration of the 10/100 Fast Ethernet interfaces. Depending on your requirements and the protocols you plan to route, you might also need to enter other configuration commands.

A Cisco device identifies a 10/100 Fast Ethernet interface by its slot number and port number, in the format slot/port. The slot/port address of a 10/100 Fast Ethernet interface on the MARC is 0/0.

The slot/port address of a 10/100 Fast Ethernet interface on the FESMIC depends upon the position of the rotary switch. For example, if the 4-port FESMIC rotary switch is in position 1, the ports are identified as 2/0, 2/1, 2/2, and 2/3. If the 2-port FESMIC rotary switch is in position 1, the ports are

identified as 2/0 and 2/1. If the 4-port FESMIC rotary switch is in position 2, the ports are identified as 3/0, 3/1, 3/2, and 3/3. If the 2-port FESMIC rotary switch is in position 2, the ports are identified as 3/0 and 3/1.

To create a basic configuration, enable, and specify IP routing on a 10/100 Fast Ethernet interface, follow these steps:

`Router>` **`enable`** `Password: password` `Router#`	Enter enable mode. Enter the password. You have entered enable mode when the prompt changes to `Router#`.
`Router#` **`configure terminal`** `Enter configuration commands, one per line.` `End with CNTL/Z.` `Router(config)#`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.
`Router#` **`ip routing`**	Enable routing protocols as required for your global configuration. This example uses IP routing.
`Router(config)#` **`interface FastEthernet`** *`0/0`* `Router(config-if)#`	Enter interface configuration mode. You have entered interface configuration mode when the prompt changes to `Router(config-if)#`.
`Router(config-if)#` **`ip address`** *`ipaddress subnetmask`*	Assign an IP address and subnet mask to the interface.
`Router(config-if)#` **`exit`**	Exit back to global configuration mode.
`Router(config)#` **`Ctrl-z`** `Router#`	When you finish configuring interfaces, return to enable mode.

Enabling the WMIC to FESMIC Connection

Unlike other Cisco 3200 Series router cards, the WMIC does not communicate with the mobile access router through the bus. It communicates through the Ethernet ports. Typically the WMIC Ethernet port is connected to a FESMIC Ethernet port. However, depending on the design, the WMIC Ethernet port might be connected to the MARC Ethernet port.

The following is an example of a configuration on the FESMIC that establishes connectivity between the WMIC and the FESMIC:

```
FESMIC#conf t
FESMIC#interface FastEthernet 2/1
FESMIC#no shut
```

The following is an example of a configuration on the WMIC that establishes connectivity between the WMIC and the FESMIC:

```
Wireless Mobile Interface Card (WMIC)#conf t
Wireless Mobile Interface Card (WMIC)#interface fastethernet 0/0
Wireless Mobile Interface Card (WMIC)#no shut
```

You can configure the serial interfaces manually by entering Cisco IOS commands on the command line.

The slot/port address of a serial interface on the SMIC depends upon the position of the rotary switch. For example, if the 4-port SMIC rotary switch is in position 1, the ports are identified as 2/0, 2/1, 2/2, and 2/3. If the 2-port SMIC rotary switch is in position 1, the ports are identified as 2/0 and 2/1. If the 4-port SMIC rotary switch is in position 2, the ports are identified as 3/0, 3/1, 3/2, and 3/3. If the 2-port SMIC rotary switch is in position 2, the ports are identified as 3/0 and 3/1

Before powering on the router, remove the serial cables from the serial ports. Otherwise when the router is powered on, if a serial cable is connected to one of the serial ports and the router does not have a valid configuration file stored in nonvolatile RAM (NVRAM), the router attempts to use the AutoInstall configuration feature to obtain a valid configuration by downloading a configuration file from the network. It can take several minutes for the process to time out.

`Router>` **`enable`** `Password:` *`password`* `Router#`	Enter privileged EXEC mode. Enter the password. You have entered enable mode when the prompt changes to `Router#`.
`Router#` **`configure terminal`** `Enter configuration commands, one per line. End with CNTL/Z.`	Enter global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.
`Router(config)#` **`ip routing`**	Enable routing protocols as required for your global configuration. This example uses IP routing.
`Router(config)#` **`interface serial`** *`1/0`* `Router(config-if)#`	Enter the interface configuration mode. You have entered interface configuration mode when the prompt changes to `Router(config-if)#`. For Cisco 3201 SMIC serial ports, slots 1, 2 and 3 are valid, and for each of these slots there are four serial ports: 0, 1, 2, and 3. For Cisco 3220 SMIC serial ports, slot 1 or 2 is valid. In the slot there are two serial ports: 0 and 1.
`Router(config-if)#` **`ip address`** *`ipaddress subnetmask`*	Assign the IP address and subnet mask to the interface.
`Router(config-if)#` **`clockrate`** *`72000`*	The router serial ports automatically detects the interface type (DTE or DCE) by the type of cable connected to the port. If you are using a port in DCE mode, connect a DCE cable and set the internal transmit clock signal (TXC) speed in bits per second. If you are using a port in DTE mode, the router automatically uses the external timing signal. You do not have to configure a clocking signal if the port is being used in DTE mode.

`Router(config-if)#` **`dce-terminal-timing-enable`**	If your serial port is DCE and the DTE side provides terminal timing (serial clock transmit external [SCTE] or terminal timing [TT]), you can use the **dce-terminal-timing-enable** command to configure the DCE to use the SCTE signal from the DTE. If the DTE side does not provide terminal timing then use the **no dce-terminal-timing-enable** command.
`Router(config-if)#` **`exit`**	Exit to global configuration mode.
`Router(config)# Ctrl-z` `Router#`	Return to privileged EXEC mode.

AUX Interface Configuration for GPS Antenna

The following is an example configuration for configuring a Global Positioning System (GPS) receiver.

```
interface Serial1/0
 ip address 20.20.0.2 255.0.0.0
!
line aux 0
 modem InOut
 transport input all
 stopbits 1
 speed 4800
!
```

The following is home agent configuration that delivers GPS data to a PC connected to the **serial 1/0** interface.

```
ip host gps 2001 20.20.0.2
!
!
interface Serial1/0
 ip address 20.20.0.3 255.0.0.0
 clock rate 125000
!
interface Serial1/1
 physical-layer async
 no ip address
!
line 3
 no motd-banner
 no exec-banner
 exec-timeout 0 0
 no flush-at-activation
 no activation-character
 no vacant-message
 modem InOut
 autocommand  telnet gps /stream
 special-character-bits 8
 transport input all
 transport output telnet
 escape-character NONE
 autohangup
 speed 4800
 flowcontrol hardware
```

View GPS Data

To view the GPS data, you can use reverse Telnet from the router.

To simulate a GPS by using Hyperterminal, do the following:

Step 1 Set the connection parameters for the COM port connecting to the router to 4800/N/8/1.

Step 2 Select hardware flowcontrol. You can see NBMA data sent from GPS. For example:

```
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215737.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*32
$GPGLL,2728.2263,S,10302.8460,W,215737.641,V*2A
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPGSV,3,1,12,29,89,000,,05,69,000,,30,56,000,,09,53,000,*77
$GPGSV,3,2,12,26,37,000,,18,35,000,,21,30,000,,06,15,000,*76
$GPGSV,3,3,12,14,15,000,,23,10,000,,07,08,000,,24,-7,000,*68
$GPRMC,215737.641,V,2728.2263,S,10302.8460,W,,,110402,,*1B
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215738.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*3D
$GPGLL,2728.2263,S,10302.8460,W,215738.641,V*25
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215738.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*0A
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215739.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*3C
$GPGLL,2728.2263,S,10302.8460,W,215739.641,V*24
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215739.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*0B
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215740.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*32
$GPGLL,2728.2263,S,10302.8460,W,215740.641,V*2A
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215740.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*05
$GPVTG,,T,,M,,N,,K*4E
```

Remote Access to the Router

The router can be accessed remotely by using applications such as Telnet. This section describes some of the remote access features.

Configure the Router to Accept a Remote Login

Use this procedure to configure the parameters that control remote access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

	Command	Purpose
Step 1	`Router(config)# line console 0`	Specifies the console terminal line.
Step 2	`Router(config-line)# exec-timeout 5`	Sets the interval that the EXEC command interpreter waits until user input is detected.
	`Router(config-line)# line vty 0 4`	Specifies a virtual terminal for remote console access

`Router(config-line)#`**`password`** *`lineaccess`*	Specifies a password on the line.
`Router(config-line)#`**`login`**	Enables password checking at terminal session login.
`Router(config-line)#` **`end`**	Exits configuration mode.

Configure the TTY Line

To configure the TTY line, do the following.

	`Router(config)#` **`line 1`**	Enter line configuration mode.
	`Router(config-line)#` **`modem inout`**	Configure a line for both incoming and outgoing calls.
	`Router(config-line)#` **`stopbits 1`**	Set the number of stop bits.
	`Router(config-line)#` **`speed`** *`38400`*	Set the baud rate.
	`Router(config-line)#` **`transport input`** *`all`*	Allow all protocols to be used when connecting to the line.
	`Router(config-line)#` **`flowcontrol`** *`hardware`*	Set the flow control.
	`Router(config-line)#` **`exit`**	Exit line configuration mode.

Access the Router with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

When the Telnet window appears, click **Connect** and select **Remote System**.

In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the device IP address.

In the Host Name field, type the device IP address and click **Connect**.

At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Secure Shell Protocol provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the home page of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/

When you connect the wireless device to the wired LAN, the it links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the Ethernet and radio ports, the network uses the BVI.

The wireless device supports only one BVI. Configuring more than one BVI might cause errors in the ARP table.

Beginning in privileged EXEC mode, follow these steps to assign an IP address to the BVI:

configure terminal	Enter global configuration mode.
interface bvi1	Enter interface configuration mode for the BVI.
ip address *address mask*	Assign an IP address and address mask to the BVI. If you are connected to the device using a Telnet session, you lose your connection to the device when you assign a new IP address to the BVI. If you need to continue configuring the device using Telnet, use the new IP address to open another Telnet session to the device.

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 3220. By using Mobile IP, you can keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

This section provides an overview of the Mobile IP technology.

Mobile IP Overview

The Cisco Mobile Networks feature enables a mobile access router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this mobile access router. Currently, this feature is a static network implementation that supports stub routers only.

In IP networks, routing is based on stationary IP addresses. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network. When a device roams away from its home network, it is no longer reachable by using normal IP routing.

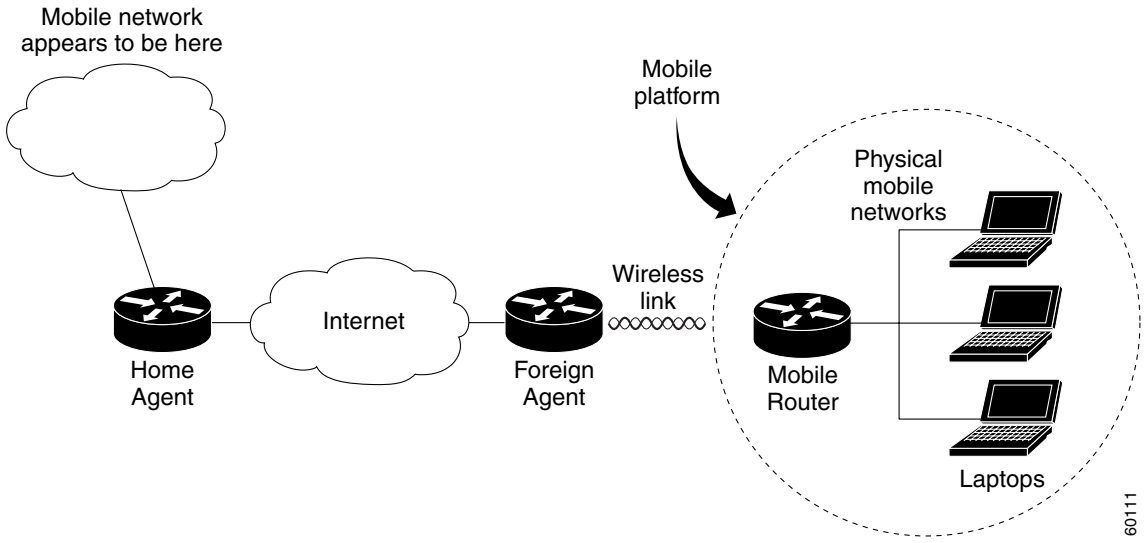
This results in the active sessions of the device being terminated. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication without sessions or connections being dropped.

Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of wireless and wire line networks while maintaining connections. Remote login, remote printing, and file transfers are examples of applications where it is desirable not to interrupt communications while an individual roams across network boundaries. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses could compromise the network services.

A device that can roam while appearing to a user to be at its home network is called a mobile node. Examples of mobile nodes include: a personal digital assistant, a laptop computer, or a data-ready cellular phone—that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain communications using the same IP address. There is no need for any changes to applications, because the solution is at the network layer, which provides the transparent network mobility.

The Cisco Mobile Networks feature comprises three components—the mobile access router (MR), home agent (HA), and foreign agent (FA). Figure 3-1 shows the three components (mobile access router, home agent, and foreign agent) and their relationships within the mobile network.

Cisco Mobile Network Components and Relationships



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

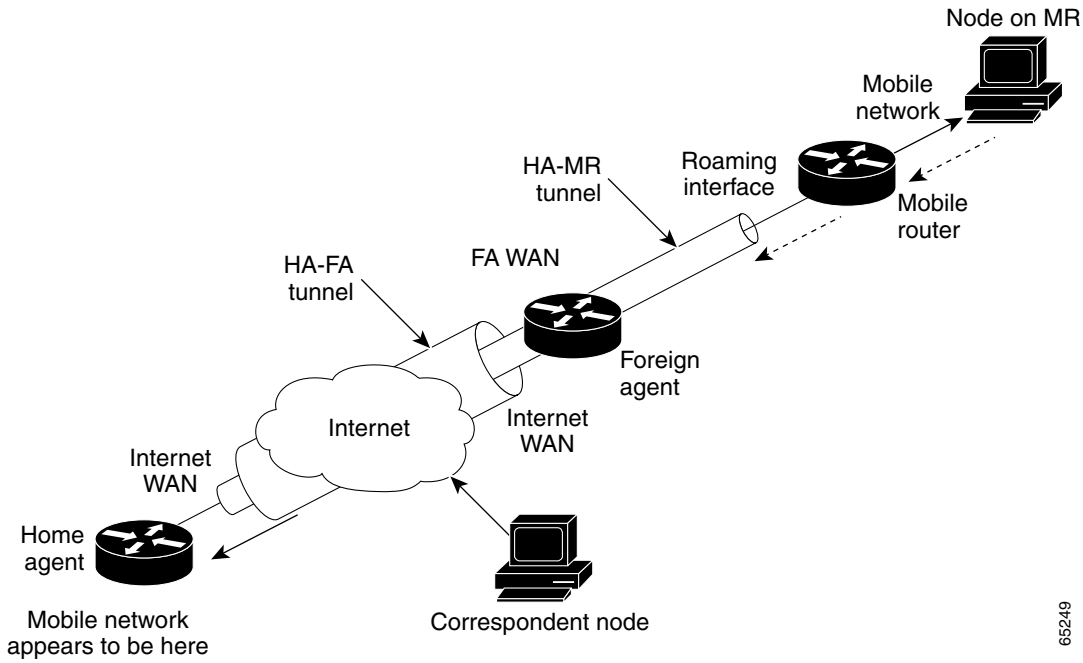
These devices can be mobile nodes without Mobile IP client software. The mobile access router eliminates the need for a Mobile IP client. The mobile access router "hides" the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

A home agent is a router on the home network of the mobile access router. It provides the anchoring point for the mobile networks. The home agent maintains an association between the home IP address of the mobile access router and its care-of address, which is the current location of the mobile access router on a foreign or visited network. The home agent is responsible for keeping track of where the mobile access router roams and tunneling packets to the current location of the mobile network. The home agent also inserts the mobile networks into its routing table.

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

Mobile IP components are shown in Figure 3-2.

Mobile IP Components and Relationships



The Mobile IP process has three main phases.

Agent Discovery—A mobile node discovers its foreign agents and home agents during agent discovery.

Registration—The mobile node registers its current location with the foreign agent and home agent during registration.

Tunneling—A reciprocal tunnel is set up by the home agent to the care-of address (current location of the mobile node on the foreign network) to route packets to the mobile node as it roams.

Agent Discovery

During the agent discovery phase, the home agent and foreign agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The mobile node listens to these advertisements to determine if it is connected to its home network or foreign network.

The IRDP advertisements carry Mobile IP extensions that specify whether an agent is a home agent, foreign agent, or both; its care-of address; the types of services it provides, such as reverse tunneling and generic routing encapsulation (GRE); and the allowed registration lifetime or roaming period for visiting mobile nodes. Rather than waiting for agent advertisements, a mobile node can send out an agent solicitation. The solicitation forces any agents on the link to immediately send an agent advertisement.

If a mobile node determines that it is connected to a foreign network, it acquires a care-of address. Two types of care-of addresses exist:

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

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

When the mobile node hears a foreign agent advertisement and detects that it has moved outside of its home network, it begins registration.

Registration

The mobile node is configured with the IP address and mobility security association (which includes the shared key) of its home agent. In addition, the mobile node is configured with either its home IP address, or another user identifier, such as a Network Access Identifier.

The mobile node uses this information along with the information that it learns from the foreign agent advertisements to form a Mobile IP registration request. It adds the registration request to its pending list and sends the registration request to its home agent, either through the foreign agent or directly if it is using a collocated care-of address and is not required to register through the foreign agent. If the registration request is sent through the foreign agent, the foreign agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported.

If the registration request is valid, the foreign agent adds the visiting mobile node to its pending list before relaying the request to the home agent. If the registration request is not valid, the foreign agent sends a registration reply with an appropriate error code to the mobile node.

The home agent checks the validity of the registration request, which includes authentication of the mobile node. If the registration request is valid, the home agent creates a mobility binding (an association of the mobile node with its care-of address), a tunnel to the care-of address, and a routing entry for forwarding packets to the home address through the tunnel.

The home agent then sends a registration reply to the mobile node through the foreign agent (if the registration request was received via the foreign agent) or directly to the mobile node. If the registration request is not valid, the home agent rejects the request by sending a registration reply with an appropriate error code.

The foreign agent checks the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the foreign agent adds the mobile node to its visitor list, establishes a tunnel to the home agent, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the mobile node.

Finally, the mobile node checks the validity of the registration reply, which includes ensuring an associated request is in its pending list as well as proper authentication of the home agent. If the registration reply is not valid, the mobile node discards the reply. If a valid registration reply specifies that the registration is accepted, the mobile node is confirmed that the mobility agents are aware of its roaming. In the collocated care-of address case, it adds a tunnel to the home agent. Subsequently, it sends all packets to the foreign agent.

The mobile node reregisters before its registration lifetime expires. The home agent and foreign agent update their mobility binding and visitor entry, respectively, during reregistration. In the case where the registration is denied, the mobile node makes the necessary adjustments and attempts to register again. For example, if the registration is denied because of time mismatch and the home agent sends back its time stamp for synchronization, the mobile node adjusts the time stamp in future registration requests.

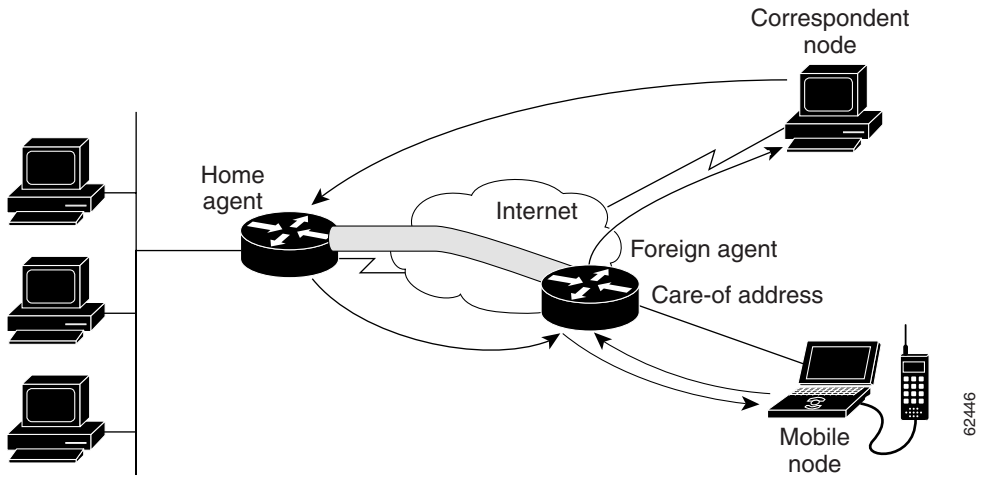
Thus, a successful Mobile IP registration sets up the routing mechanism for transporting packets to and from the mobile node as it roams.

Tunneling

The mobile node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the mobile node is roaming on foreign networks, its movements are transparent to correspondent nodes.

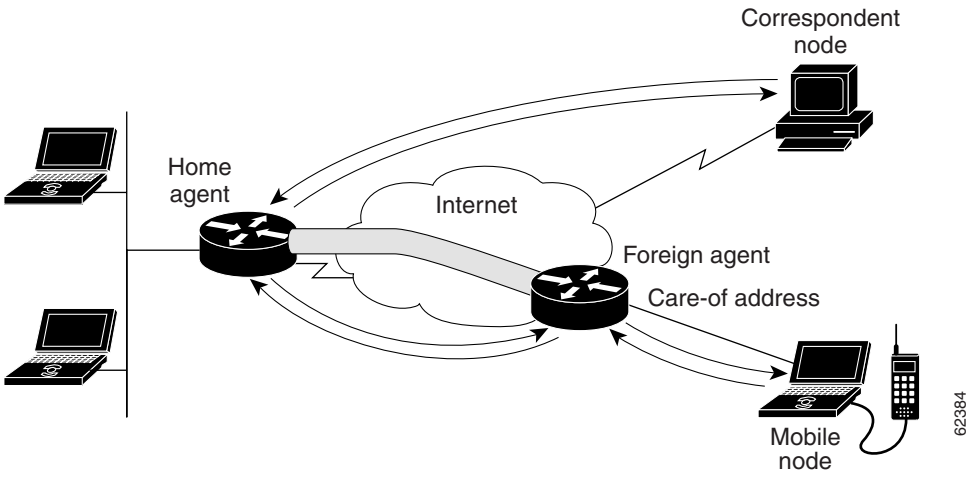
Data packets addressed to the mobile node are routed to its home network, where the home agent now intercepts and tunnels them to the care-of address toward the mobile node. Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The default tunnel mode is IP Encapsulation within IP Encapsulation. Optionally, GRE within IP can be used.

Typically, the mobile node sends packets to the foreign agent, which routes them to their final destination, the Correspondent Node, as shown in Figure 3-3.



However, this data path is topologically incorrect because it does not reflect the true IP network source for the data—rather, it reflects the home network of the mobile node. Because the packets show the home network as their source inside a foreign network, an access control list on routers in the network called ingress filtering drops the packets instead of forwarding them. A feature called reverse tunneling solves this problem by having the foreign agent tunnel packets back to the home agent when it receives them from the mobile node. See Figure 3-4.

Reverse Tunnel



Tunnel MTU discovery is a mechanism for a tunnel encapsulator such as the home agent to participate in path MTU discovery to avoid any packet fragmentation in the routing path between a correspondent node and mobile node. For packets destined to the mobile node, the home agent maintains the MTU of the tunnel to the care-of address and informs the correspondent node of the reduced packet size. This improves routing efficiency by avoiding fragmentation and reassembly at the tunnel endpoints to ensure that packets reach the mobile node.

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

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

Dynamic Host Configuration Protocol (DHCP) is commonly used in corporate environments. DHCP allows a server to dynamically assign IP addresses and to deliver configuration parameters to nodes. The DHCP Server verifies the identity of the node, leases it the IP address from a pool of addresses for a predetermined period of time, and reclaims the address for reassignment when the lease expires. The node can terminate existing communication sessions, move to a new point of attachment to the network, reconnect to the network, and receive a new IP address from DHCP. This conserves IP addresses and reduces Internet access costs. However, if users are mobile and need continuous communications and accessibility, DHCP is not an adequate solution. DHCP does not allow applications to maintain connections across subnet-to-network boundaries. Mobile IP does not drop the network prefix of the IP address of the node, which is critical to the proper routing of packets throughout the Internet, and providing continuous connectivity.

Basic Home Agent and Foreign Agent Configurations

This chapter describes:

Home Agent and Foreign Agent Configuration

To enable Mobile IP services on your network, you must determine which home agents will facilitate the tunneling for selected IP address, and where these devices or router will be allowed to roam. The areas, or subnets, into which the hosts are allowed to roam determine where foreign agent services need to be set up.

Configure your foreign agent routers:

Enabling Foreign Agent Mobile IP and Services

Verifying Foreign Agent Configuration

Configure your home agent routers:

Enabling Home Agent Mobile IP

Verifying Home Agent Configuration

Note For a complete description of the Mobile IP commands, refer to the “Mobile IP Commands” chapter of the *Cisco IOS IP and IP Routing Command Reference* publication.

Enabling Foreign Agent Mobile IP and Services

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

	Command	Purpose
Step 1	`Router(config)# router mobile`	Enables Mobile IP on the router.
Step 2	`Router(config)# ip mobile foreign-agent care-of` *interface*	Enables foreign agent services when at least one care-of address is configured. This is the foreign network termination point of the tunnel between the foreign agent and home agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.
Step 3	`Router(config)# interface` *type number*	Configures an interface and enters interface configuration mode.
Step 4	`Router(config-if)# ip address` *ip-address mask*	Configures a primary IP address of the interface.
Step 5	`Router(config-if)# ip irdp`	Enables ICMP Router Discovery Protocol (IRDP) processing on an interface.
Step 6	`Router(config-if)# ip irdp maxadvertinterval` *seconds*	(Optional) Specifies maximum interval in seconds between advertisements.
Step 7	`Router(config-if)# ip irdp minadvertinterval` *seconds*	(Optional) Specifies minimum interval in seconds between advertisements.
Step 8	`Router(config-if)# ip irdp holdtime` *seconds*	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the **maxadvertinterval** period.
Step 9	`Router(config-if)# ip mobile foreign-service`	Enables foreign agent service on an interface. This will also append Mobile IP information such as care-of address, lifetime, and service flags to the advertisement.

Example of a Foreign Agent Router Configuration

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

```
router mobile
ip mobile foreign-agent care-of serial1/0
!
interface serial1/0
 ip address
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 ip mobile foreign-service
```

Enabling Home Agent Mobile IP

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

To enable Mobile IP on a home agent router, enter the following commands:

	Command	Purpose
Step 1	Router(config)#**router mobile**	Enables Mobile IP on the router.
Step 2	Router(config)#**ip mobile home-agent**	Enables Home Agent Service.
Step 3	Router(config)#**ip mobile virtual-network** *net mask* [**address** *address*]	Adds virtual network to routing table. If not using a virtual network, go to Step 6.
Step 4	Router(config)# **router** *protocol*	Configures a routing protocol.
Step 5	Router(config)# **redistribute mobile**	Enables redistribution of a virtual network into routing protocols.
Step 6	Router(config)# **ip mobile host** *lower* [*upper*] [**interface** *name* | **virtual-network**] *net mask* [**lifetime** *number*]	Configures the mobile access router as the mobile host. The IP address is in the home network. The **interface** *name* option configures a physical connection from the home agent to the mobile access router.
Step 7	Router(config)# **ip mobile mobile-networks** *ip-address*	Configures mobile networks on the mobile host and enters mobile networks configuration mode.
Step 8	Router(mobile-networks)# **description** *string*	(Optional) Adds a description to a mobile access router configuration.
Step 9	Router(mobile-networks)# **network** *net mask*	Specifies a list of networks for the mobile access router routing process.
Step 10	Router(mobile-networks)# **exit**	Exits mobile networks configuration mode.
Step 11	Router(config)# **ip mobile secure host** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*	Sets up mobile host security associations. The SPI and key between the Home Agent and mobile access router are known. The address is the home IP address of the mobile access router.

Example of a Home Agent Configuration

In the following example, the home agent has five mobile hosts on interface Ethernet1 (network 11.0.0.0) and ten on virtual network 10.0.0.0. There are two mobile node groups. Each mobile host has one security association. The home agent has an access-list to disable roaming capability by mobile host 11.0.0.5.

The 11.0.0.0 group has a lifetime of 1 hour (3600 secs). The 10.0.0.0 group cannot roam in areas where the network is 13.0.0.0.

```
router mobile
```

```
!
! Define which hosts are permitted to roam
ip mobile home-agent broadcast roam-access 1
!
! Define a virtual network
ip mobile network 10.0.0.0 255.0.0.0
!
! Define which hosts are on the virtual network, and the care-of access list
ip mobile host 10.0.0.1 10.0.0.10 virtual-network 10.0.0.0 255.0.0.0 care-of-access 2
!
! Define which hosts are on Ethernet 1, with lifetime of one hour
ip mobile host 11.0.0.1 11.0.0.5 interface Ethernet1 lifetime 3600
!
! The next ten lines specify security associations for mobile hosts
! on virtual network 10.0.0.0
!
ip mobile secure host 10.0.0.1 spi 100 key hex 12345678123456781234567812345678
ip mobile secure host 10.0.0.2 spi 200 key hex 87654321876543218765432187654321
ip mobile secure host 10.0.0.3 spi 300 key hex 31323334353637383930313233343536
ip mobile secure host 10.0.0.4 spi 100 key hex 45678332353637383930313233343536
ip mobile secure host 10.0.0.5 spi 200 key hex 33343536313233343536373839303132
ip mobile secure host 10.0.0.6 spi 300 key hex 73839303313233343536313233343536
ip mobile secure host 10.0.0.7 spi 100 key hex 83930313233343536313233343536373
ip mobile secure host 10.0.0.8 spi 200 key hex 43536373839313233330313233343536
ip mobile secure host 10.0.0.9 spi 300 key hex 23334353631323334353637383930313
ip mobile secure host 10.0.0.10 spi 100 key hex 63738393132333435330313233343536
!
! The next five lines specify security associations for mobile hosts
! on Ethernet1
!
ip mobile secure host 11.0.0.1 spi 100 key hex 73839303313233343536313233343536
ip mobile secure host 11.0.0.2 spi 200 key hex 83930313233343536313233343536373
ip mobile secure host 11.0.0.3 spi 300 key hex 43536373839313233330313233343536
ip mobile secure host 11.0.0.4 spi 100 key hex 23334353631323334353637383930313
ip mobile secure host 11.0.0.5 spi 200 key hex 63738393132333435330313233343536

!
! Deny access for this host
access-list 1 deny   11.0.0.5
!
! Deny access to anyone on network 13.0.0.0 trying to register
access-list 2 deny   13.0.0.0
```

Monitoring and Maintaining Mobile IP

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

Command	Purpose
`Router# show ip mobile binding`	Displays mobility bindings (home agent only).
`Router# show ip mobile tunnel`	Displays active tunnels.
`Router# show ip mobile visitor`	Displays visitor bindings (foreign agent only).
`Router# show ip route mobile`	Displays Mobile IP routes.
`Router# show ip mobile traffic`	Displays protocol statistics.
`Router# show ip mobile violation`	Displays information about security violations.
`Router# debug ip mobile advertise`	Displays advertisement information.[1]
`Router# debug ip mobile host`	Displays mobility events.

1. Make sure IRDP is running on the interface.

Verifying Home Agent Configuration

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

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

Verifying Foreign Agent Configuration

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

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

To clear the mobile access router statistics, use the following commands in privileged EXEC mode:

`Router# clear ip mobile router agent`	Deletes learned agents and the corresponding care-of address of the foreign agent from the mobile access router agent table.
`Router# clear ip mobile router registration`	Deletes registration entries from the mobile access router registration table.
`Router# clear ip mobile router traffic`	Clears the counters that the mobile access router maintains.

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

`Router(config)# no ip mobile home-agent`	Disables home agent services.
`Router(config)# no ip mobile foreign-agent`	Disables foreign agent services.
`Router(config)# no router mobile`	Stops Mobile IP process.

Setup Router Configuration Utility

Setup (also known as the System Configuration Dialog) is an interactive CLI mode that guides you through first-time configuration by prompting you for the details needed to start your router functioning in the network. While Setup mode is a quick and easy way to perform first-time configuration of a router, you can also use it after first-time startup to perform basic configuration changes.

Before using Setup, you should have the following information so that you can configure the system properly:

- Which interfaces you want to configure
- Which routing protocols you wish to enable
- Whether the router is to perform bridging
- Network addresses for the protocols being configured
- Password strategy for your environment

Note Refer to the documentation for your particular hardware platform for information on how you should use Setup for first-time startup. For a complete description of the **setup** command, refer to the "Using the Setup Configuration Tool" chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the *Cisco IOS Command Reference Master Index* or search online.

Using Setup After First-Time Startup

The CLI allows you to make very detailed changes to your system configuration. However, some major configuration changes do not require the granularity provided by the CLI. You can use Setup to configure general characteristics of the system. For example, you might want to use Setup to add a protocol suite, to make major addressing scheme changes, or to configure a newly installed interface. Although you can use the configuration modes available though the CLI to make these changes, the Setup mode provides you with a high-level view of the configuration and guides you through the configuration process.

If you are not familiar with Cisco products and the CLI, Setup is a particularly valuable tool because it prompts you for the specific information required to configure your system.

Note If you use Setup to modify a configuration because you have added to or modified the hardware, be sure to verify the physical connections using the **show version** EXEC command. Also, verify the logical port assignments using the **show running-config** EXEC command to ensure that you configure the proper port. Refer to the hardware documentation for your platform for details on physical and logical port assignments.

To enter Setup mode, use the following command in privileged EXEC mode:

Command	Purpose
`Router# setup`	Enters Setup mode.

When you enter the **setup** EXEC command after first-time startup, an interactive dialog called the *System Configuration Dialog* appears on the system console screen. The System Configuration Dialog guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt reflect either the default settings or the last configured setting.

You must progress through the System Configuration Dialog until you come to the item that you intend to change. To accept default settings for items that you do not want to change, press the Return or Enter key. The default choice is indicated by square brackets (for example, [yes]) before the prompt colon (:).

To exit Setup and return to privileged EXEC mode without making changes and without progressing through the entire System Configuration Dialog, press **Ctrl**-**C**.

The facility also provides help text for each prompt. To access help text, press the question mark (**?**) key at a prompt.

When you complete your changes, the system will automatically display the configuration file that was created during the Setup session. It also asks you if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM as the startup configuration file. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

In the following example Setup is used to configure interface serial 1/1 and to add ARAP and IP PPP support on the asynchronous interfaces. Note that prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed in the device.

```
Router# setup

         --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

Interface          IP-Address      OK?  Method    Status                  Protocol
FastEthernet0/0    172.16.72.2     YES  manual    up                      up
Serial1/0          unassigned      YES  not set   administratively down  down
Serial1/1          172.16.72.2     YES  not set   up                      up
Serial1/2          unassigned      YES  not set   administratively down  down
Serial1/3          unassigned      YES  not set   administratively down  down

Configuring global parameters:

  Enter host name [Router]:

The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.


Enter enable secret [<Use current secret>]:

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password [ww]:
  Enter virtual terminal password [ww]:
```

```
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure DECnet? [no]:
  Configure AppleTalk? [yes]:
    Multizone networks? [no]: yes
  Configure IPX? [yes]: no
  Configure IP? [yes]:
    Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [15]:
  Configure Async lines? [yes]:
    Async line speed [9600]: 57600
    Configure for HW flow control? [yes]:
    Configure for modems? [yes/no]: yes
      Configure for default chat script? [yes]: no
    Configure for Dial-in IP SLIP/PPP access? [no]: yes
      Configure for Dynamic IP addresses? [yes]: no
      Configure Default IP addresses? [no]: yes
      Configure for TCP Header Compression? [yes]: no
      Configure for routing updates on async links? [no]:
    Configure for Async IPX? [yes]: no
    Configure for Appletalk Remote Access? [yes]: no


Configuring interface parameters:
!
!...
!

The following configuration command script was created:
!
!...
```

5

Wireless LAN Example Scenario

The wireless LAN relies on high-speed wireless *hot spots*. Unlike public hot spots —which have begun to appear in airports, hotel lobbies, and coffee shops, allowing anyone with a wireless-enabled computer or PDA to access the Internet—the hot spots used by police, firefighters, and paramedics are secure and accessible only to authorized personnel.

High-speed wireless LANs can send and receive live video feeds, known as IP video. This technology can be used to monitor public areas from remote locations and to gain insight into rapidly developing or escalating situations. Incident commanders can view structure fires, protests, and other events as they're happening, helping them to direct response teams and resources accordingly.

A 911 dispatcher can send a police helicopter to the scene of a fire, giving emergency services personnel a better idea of the resources needed to control the situation, to save lives, save property, and gather evidence. It also helps various agencies coordinate resources.

On the ground, ambulances can transmit live video and data, allowing medical teams to observe the condition of patients before they arrive. Police can monitor areas of concern without actually driving there, preserving the safety of emergency personnel. Officers can view fellow officers as they make traffic stops and respond to disturbances, instead of simply retrieving videotape from a cruiser after something has gone wrong.

High-speed wireless LAN coverage can be limited to one or two hot spots measuring a few hundred feet in diameter, or a wireless LAN can be extended across an entire community by using multiple overlapping hot spots.

802.11 wireless technology is attractive to many municapalities because deployment can begin with the establishment of hot spots around police stations and firehouses, and expanded to other areas as resources become available and utilization increases.

At the center of each hot spot is a devices known as an access points, which can be connected to a wired or a wireless network to create secure wireless gateways, enabling authorized personnel to send and receive data using wireless-enabled notebooks, PDAs, and other devices. And 802.11 wireless technology is now portable as a result of recent developments at Cisco Systems, Inc.

A vehicle can be equipped with a router, a bridge, and an access point. The bridge provides wireless communications with the municipal LAN. The access point communicates with devices that would otherwise be out of range of a fixed hot spot. The router manages fast, reliable communications between the local devices and the municipal LAN.

Silicon Beach Police Example Scenario

The mission is for Silicon Beach Police to extend its mobility, increase work efficiency, and improve the quality of its services to the public.

Until recently, when police respond to a robbery, they have no idea what to expect when they get there. This lack of information is a major disadvantage. However, with an IP video surveillance solution, that is no longer the case. When an alarm is triggered at the scene of a robbery, the existing security cameras transmit the video over a network of wireless routers, bridges, and access points.

Police officers can see what is happening inside the bank from any wireless hot spot. Emergency vehicles can become mobile wireless hot spots, maintaining high-speed connections while in motion, allowing officers to make faster, better, safer decisions.

Without this technology, police must rely on witnesses, limited observations made from outside the building, and voice descriptions. With this technology, police can see inside a building in real time. As a result, the incident is more likely to be brought to a conclusion with a minimum risk of injury, loss of life, or loss of property.

Without this technology, a suspect is typically transported to headquarters to be photographed and fingerprinted by police technicians, who must manually compare the results to relevant databases. A wireless LAN in the officer's cruiser connected to the municipal LAN enables the officer to conduct a real-time database query on the suspect, verifying the suspect's identity, but could lead to a match with information from an unsolved case.

Objective

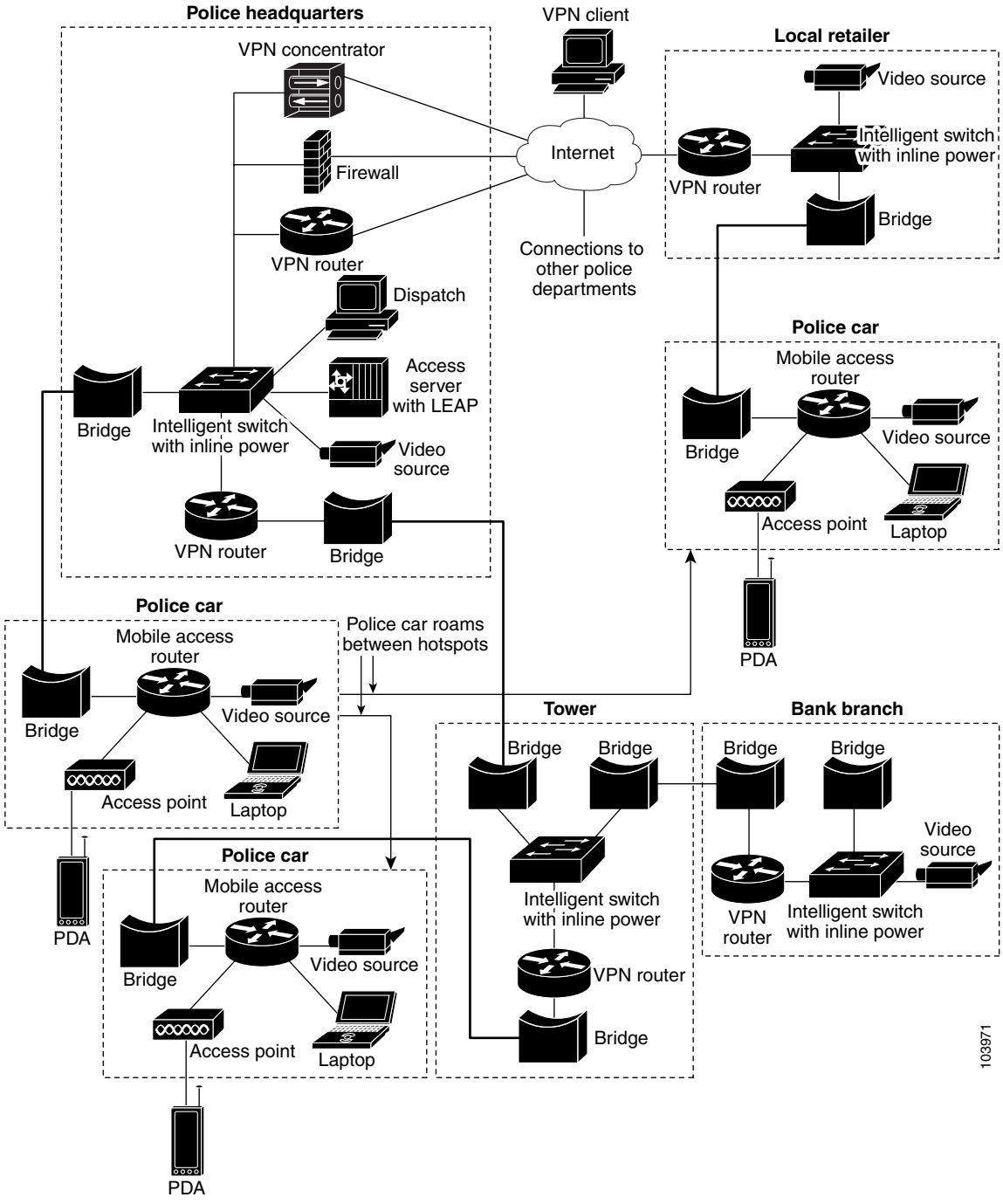
To provide a mobile wireless solution that enables Silicon Beach Police to obtain a seamless, continuous network connections with other wireless and wired network services. The recommended solution meets the following requirements:

- Seamless, continuous wireless connections from the police vehicle to the home network.
- Streaming real-time video across the network, including headquarters and other police vehicles.
- End to end security

Approach

Create Mobile IP hotspots that allow the router to connect to the home network while the emergency vehicles are mobile. Figure 5-1 shows the Cisco Mobile IP home network at police headquarters, and foreign agent hotspots.

Figure 5-1 Configuration Overview



There are four hotspots:

- police department headquarters
- bank
- retail establishment
- traffic light, used as a tower

Silicon Beach Police includes a secure connection to other emergency services, such as the fire department, through the Internet by using a VPN tunnel. Each hotspot contains an Access Point that communicates with the wireless workgroup bridge inside the police vehicles to provide network connectivity to these police vehicles. The setup includes:

- Video cameras mounted at the bank and police stations
- Video servers that can record and archive
- Alarm Triggered Internet Protocol

Silicon Beach Police Officers in properly equipped cruisers can view real-time video of a crime scene on their laptops as soon as an alarm is triggered, and respond according to what they see occurring. The video feeds are also accessible on Personal Digital Assistants (PDAs), providing even greater intelligence gathering flexibility.

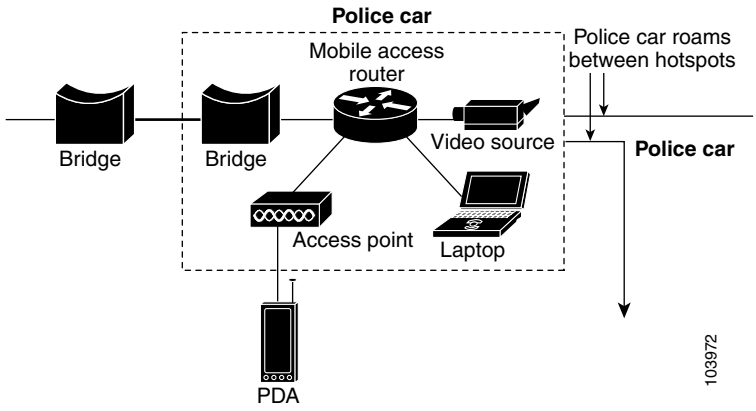
A camera mounted on the dashboard of the police cruiser is connected to the municipal LAN. The live image can be viewed by authorized personnel from anywhere in the Silicon Beach Police network, including headquarters, a mobile command center, or other police vehicles.

Security is implemented in two forms: VPN and LEAP. VPN tunnels secure the data in both the wired and wireless networks. Security between a cruiser and a foreign agent, such as the bank, is supported by the wireless device. LEAP authenticate devices to an ACS server in the home network. When a client, such as a personal computer, associates with the access point on the cruiser, the personal computer is authenticated before any traffic is allowed through the access point.

The hardware and software components in each mobile police unit include:

- One Cisco 3220 Series Mobile Access Router with two Cisco 3201 Wireless Mobile Interface Cards, one configured to be an access point and the other as a wireless workgroup bridge.
- One analog camera
- One video server (IP out)
- A laptop personal computer with viewing software

Figure 5-2 shows the police car configuration. Note that the wireless workgroup bridge and the access point are attached to and draw power from the router.



The bridge links the cruiser mobile access router to the larger municipal LAN. The bridge and the access point connect to the router through internal Ethernet connections. The router can be connected to the remaining LAN devices by using wireless connections, Ethernet ports, or serial ports. Depending on the configuration, the access point could associate with devices in other vehicles.

Police Cruiser Cisco 3200 Mobile Access Router Configuration Example

The Ethernet port on each WMIC is connected to Ethernet ports on the FastEthernet switch card or the Ethernet port on one WMIC might be connected to the Ethernet port on the mobile access router card. We recommend that the WMIC Ethernet ports be connected to the FastEthernet switch card. However, your configuration might be different, depending on how your system integrator assembled the router.

Typically these connections are made internally. These links provide communications between the WMICs and the router. It is not necessary to make a similar connection between the FastEthernet switch card and the mobile access router card, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
no spanning-tree vlan 1
!
ip dhcp excluded-address 192.168.100.5
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool MobileNetwork
  network 192.168.100.0 255.255.255.0
  default-router 192.168.100.1
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 60.1.1.2
!
crypto isakmp peer address 60.1.1.2
!
crypto ipsec transform-set testtrans ah-md5-hmac esp-aes 256 esp-sha-hmac comp-lzs
!
crypto map ToSecureNet 10 ipsec-isakmp
 set peer 60.1.1.2
 set transform-set testtrans
 match address 155
```

```
!
interface Loopback1
 ip address 66.1.1.5 255.255.255.0
 crypto map ToSecureNet
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
 ip policy route-map SecureNetPolicy
 description Connection_to_Access_Point
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
!
interface FastEthernet2/1
 no ip address
 shutdown
!
interface FastEthernet2/2
 no ip address
 shutdown
!
interface FastEthernet2/3
 descriptiong WMIC_WGB_Connection
 no ip address
!
interface Vlan1
 ip address 70.70.70.2 255.255.255.0
 ip mobile router-service roam priority 255
 ip mobile router-service solicit interval 1
!
ip local policy route-map SecureNetPolicy
!
access-list 155 permit ip 192.168.100.0 0.0.0.255 any
!
route-map SecureNetPolicy permit 10
 match ip address 155
 set interface Loopback1
!
router mobile
!
ip mobile secure home-agent 200.200.200.1 spi 100 key hex 12345678123456781234567812345678
algorithm md5 mode prefix-suffix
!
ip mobile router
  address 65.1.1.5 255.255.255.0
  home-agent 200.200.200.1
  reverse-tunnel
```

Police Cruiser Wireless Workgroup Bridge Configuration Example

One Ethernet port on the WMIC connects the card configured as a workgroup bridge to an Ethernet port on either the FastEthernet switch card or the mobile access router card. Typically this connection is made internally, and provides communications between the WMIC being used as a workgroup bridge and the router.

If the connection is made to the FastEthernet switch card, is not necessary to connect the FastEthernet switch card to the mobile access router card by using the FastEthernet ports, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 1 size 128bit 0 12345678901234567890123456 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_hotspot
    infrastructure-ssid
 !
 cca 0
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 power local cck maxmimum
 power local ofdm maximum
 power client maximum
 station-role workgroup-bridge
 mobile station
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address dhcp
 no ip route-cache
!
ip radius source-interface BVI1
bridge 1 route ip
```

Police Car Access Point Configuration Example

One Ethernet port on the WMIC connects the card configured as an access point to an Ethernet port on either the FastEthernet switch card or the mobile access router card. Typically this connection is made internally. This link provides communications between the WMIC being used as an access point and the router.

If the connection is made to the FastEthernet switch card, is not necessary to connect the FastEthernet switch card to the mobile access router card by using the FastEthernet ports, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 2 size 128bit 0 12345678901234567890123456 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_wep
    authentication open
    infrastructure-ssid
 !
 cca 0
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 power local cck maximum
 power local ofdm maximum
 power client maximum
 channel least-congested
 station-role root ap-only
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.100.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.100.1
!
ip radius source-interface BVI1
bridge 1 route ip
```

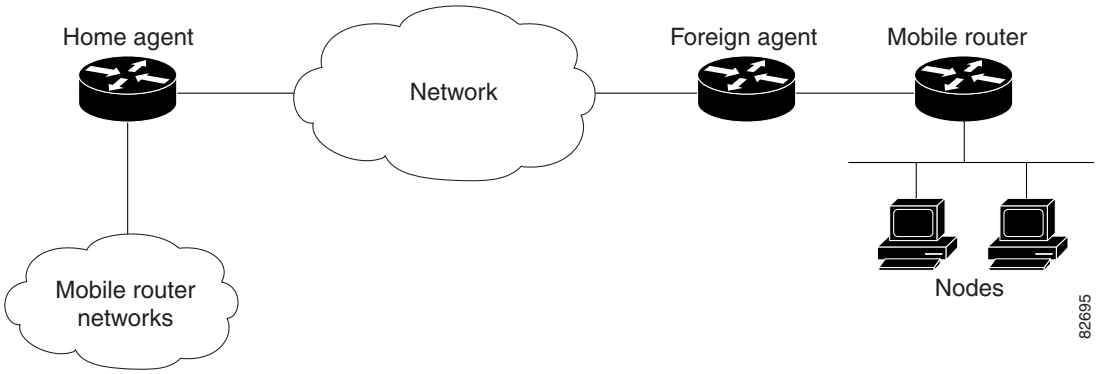
Static and Dynamic Network Configuration

This chapter describes:

Static Networks

The mobile access router can be part of a static network or a dynamic network. A static network supports stub routers only and allows a mobile access router to roam about, behaving like a mobile node. The home agent treats this mobile node as a mobile access router. The home agent adds the mobile access router networks to the routing table when the mobile access router is registered.

Figure 6-1 Basic Mobile Access Router Configuration



The home agent functionality consists of the following:

- When the mobile access router is registered, mobile access router networks are added to the routing table and a tunnel interface between home agent and mobile access router is created
- Packets destined for mobile access router networks are encapsulated by the home agent

Mobile access router functionality consists of the following:

- Configuration of the home agent address and registration parameters, as well as the interfaces used for roaming
- Agent solicitation, if configured
- Registers to its home agent (retransmit if no reply received)
- Registers when a better interface comes up
- Re-registers before the lifetime expires

When the mobile access router is brought up, it is in unknown state. After it receives agent advertisements, it determines if it is at its home or away from its home. It is at home when the source of the advertisement is on its home network, and it behaves like a normal router. When the mobile access router is roaming, it does not send any routing updates on its roaming interfaces. It sends a registration request through the learned foreign agent, to its home agent.

After mobile access router sends registration request, it goes into Pending state. If the registration is accepted by the home agent, the mobile access router is registered. If registration is denied, the mobile access router tries to register through another foreign agent.

Table 6-1 shows the states of the mobile access router.

Table 6-1 Mobile Access Router States

State	Description
Home	Connected to home network.
Registered	Registered on foreign network.
Pending	Sent registration request and is waiting for the reply.
Isolated	Isolated from network.
Unknown	Can not determine its state.

Agent advertisements are ICMP Router Discovery Protocol (IRDP) messages which convey Mobile IP information. The advertisement contains the IRDP lifetime (the number of seconds that agent is considered valid). It also contains the care-of address (CoA), the point of attachment on foreign network, and supported services such as Generic Routing Encapsulation (GRE) , reverse tunnel, and so forth.

There are two modes of operation:

- Periodic advertisements by agents
- Periodic solicitations by mobile access router

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

For periodic solicitations, the IRDP lifetime is 0. The mobile access router sends solicitations based on the user configured interval. If no advertisement is heard after a period of 3 times the interval, the mobile access router considers that agent to be disconnected.

When does mobile access router send out agent solicitations?

To learn about foreign agents quickly, the mobile access router sends agent solicitations when the roaming interface comes up or when the interface is configured for roaming. Otherwise, the mobile access router only sends agent solicitations when it is configured for periodic solicitation.

What does mobile access router do when it hears an agent advertisement?

It gathers two pieces of information: agent availability and registration service. The mobile access router maintains an agent table containing a list of active agents. This is used to decide which agent with which to register. When the mobile access router registers, it fills in the request with CoA, lifetime, and service flags based on the received advertisement. If there are multiple CoAs, the mobile access router uses the first one in the advertisement.

Note The agent advertisement includes the IRDP lifetime and the registration lifetime. The IRDP lifetime indicates to the mobile access router how long the advertisement is valid. The registration lifetime specifies the duration of a registration for which mobile access router can attempt to register.

How does mobile access router decide which agent to use?

The mobile access router maintains an agent table based on received advertisements. Since only one agent is active, either the mobile access router is registered through a foreign agent or it is at home, connected to its home agent. The mobile access router chooses the agent by using the following criteria:

- Agents heard on same interface, the mobile access router selects most recently heard agent
- Agents heard on different interfaces, the mobile access router selects agent on preferred interface

When does mobile access router send registration request?

The mobile access router sends registration requests to the active foreign agent. The following events trigger a request:

- When movement from one foreign agent to another is detected
- A foreign agent reboot is detected
- The mobile access router is isolated and hears a foreign agent
- A better foreign agent is learned
- Active foreign agent ages out and other foreign agents exist
- Re-registration of an active session
- Recovery from denials due to mismatched ID (133) or lifetime too long (68)
- The hold down period for a foreign agent expires
- The interface connected to an active foreign agent goes down while other foreign agents exist
- The mobile access router configuration (registration lifetime, home agent address) changes

When does mobile access router delete agent from table?

The mobile access router removes the learned agent from the table when:

- An agent advertisement ages out
- An active foreign agent does not respond to a registration request
- A denied registration reply which is not mismatched ID (133) nor lifetime too long (68) is received
- The interface where the agent was learned goes down
- Roaming on an interface where the agent was learned is deconfigured
- A user deconfigures the mobile access router
- A user manually clears an agent by using the command line interface

Timers

There are 5 timers: agent solicitation, agent advertisement, registration, lifetime, and hold down.

The agent solicitation timer is for the periodic transmission of solicitations. By default, the timer is off. But if an interface is configured for solicitation, the mobile access router solicits advertisements until an advertisement is received. Then the mobile access router sends solicitations at regular intervals.

The agent advertisement timer is for aging out received advertisements. When advertisement is received, the timer is started based on the IRDP lifetime. As subsequent advertisements arrive, the mobile access router restarts the timer. When the timer expires, it means agent has not been heard for awhile, and the agent is removed from the table.

The registration timer sets the periodic transmission of registration requests. The mobile access router registers when this timer expires. It attempts to register until a reply is received. Then the mobile access router sends a request before the registration lifetime expires.

The registration lifetime timer is used for aging out registration when the lifetime has expired. When it is accepted, registration reply is received, and the timer is started based on granted lifetime. As subsequent replies arrive, the mobile access router restarts the timer. When the timer expires, the registration is deleted.

The hold down timer expires when an interface is no longer in hold down mode. By default, the timer is off. But if the interface is configured for hold down, the mobile access router waits for timer to expire before using agents learned on the interface.

Preferred Path

The mobile access router sets a preference for an agent based on which interface the advertisement received. If more than one interface receives agent advertisements, the one with higher roaming priority value is preferred. If multiple interfaces have the same priority, the highest bandwidth is preferred. If interfaces have same bandwidth, the highest interface IP address is preferred. The mobile access router send registration requests to the preferred foreign agent and deregistration to preferred home agent.

Hold Down

The mobile access router waits for the hold down period to expire before using an agent. This avoids prematurely registering to a better agent on a weak wireless link. The mobile access router makes sure that link is reliable for a period of time before committing to using that agent.

Registration

After agent discovery, the mobile access router registers with an foreign agent or deregisters to its home agent. When mobile access router is in a foreign network, it can register in one of the following modes:

- Foreign agent CoA
- Collocated CoA

The foreign agent CoA mode is when mobile access router sends a registration request (using advertised CoA) to a foreign agent, which relays a request to the home agent, which process it and sends a reply back to the foreign agent, which relays reply to mobile access router. The routing path between the home agent and the foreign agent (CoA) is set up after registration is successful.

The collocated care-of address (CCoA) mode is when mobile access router gets an address in the foreign network and sends a registration request (using the address assigned to the mobile access router as collocated CoA) directly to the home agent, which process it and sends a reply back to mobile access router. The routing path between the home agent and the mobile access router (collocated CoA) is set up after registration is successful.

When the mobile access router detects that it is at home, it sends a deregistration request to its home agent.

The following events trigger a registration:

- A foreign agent advertisement is received, and the mobile access router has a reason to register
- An active foreign agent advertisement (IRDP lifetime) expired, and the mobile access router chooses another learned foreign agent to register
- The registration timer expired due to the retransmission or lifetime aging
- Recovery from the home agent, which replied with a denial due to a mismatched ID
- Recovery from a foreign agent, which replied with a denial due to lower lifetime
- After mobile access router configuration, the mobile access router has enough information and reason to register with the most reliable foreign agent

The reasons registration is needed are as follows:

- Movement is detected
- A foreign agent reboot detected
- The mobile access router is isolated
- A better interface has a reliable foreign agent
- The mobile access router is on foreign network without an active foreign agent
- The mobile access router is on home network when it has active foreign agent

When a registration reply is received, the mobile access router processes it if the home address field equals its own home address. The mobile access router finds the request in the registration table that corresponds to the reply. It authenticates the reply and sets up a routing path between the home agent and the mobile access router. Also, it creates a default route through the foreign agent.

Routing

There is a tunnel between the home agent and the CoA, and another tunnel between the home agent and the mobile access router.

How do packets reach devices on mobile networks?

On the mobile access router, there is one tunnel between the home agent and the mobile access router. Packets from the home agent that arrive at the mobile access router through the tunnel are decapsulated and forwarded to the destination device on the mobile access router mobile network.

How are packets from devices on mobile networks routed?

By default, the mobile access router creates a default route through the foreign agent. So packets from devices arrive at the mobile access router, and it forwards the packets to the foreign agent by default, based on a routing decision. Routing fails if networks between the endpoints have ingress filtering that drops topologically incorrect packets or the mobile network uses private addresses.

Using a reverse tunnel, the mobile access router creates a default route through the tunnel, between the home agent and the mobile access router and a host route to the home agent through the foreign agent. So packets from devices arrive at the mobile access router, that encapsulates the packets before sending them to the foreign agent. Reverse tunnel using direct delivery style is supported. This results in packets going back to mobile access router home network, though ingress filtering is avoided and a private mobile network can be supported.

How are routing protocols affected?

When the mobile access router is at home, all routing protocols behave normally. When mobile access router is roaming, it does not propagate any routes out interfaces that are configured for roaming.

Can mobile network be split?

First, we advised that the mobile network exist on one non-roaming interface of the mobile access router. In the unavoidable case where mobile network is on a roaming interface, it is mandatory that all nodes exist on the mobile network of the mobile access router and that none exist on the home agent. Otherwise, the routing table on the mobile access router prevents communications between nodes, that are disjointed (one on the home agent and one on the mobile access router) while roaming. The mobile access router has a connected route to the mobile network and forwards packets out of its interface.

Home Agent Component

The additional information a home agent needs for a mobile host that supports mobile networks is which networks should be injected into the routing table when registered.

The following data structures are needed:

- Mobile network group
- Mobile network

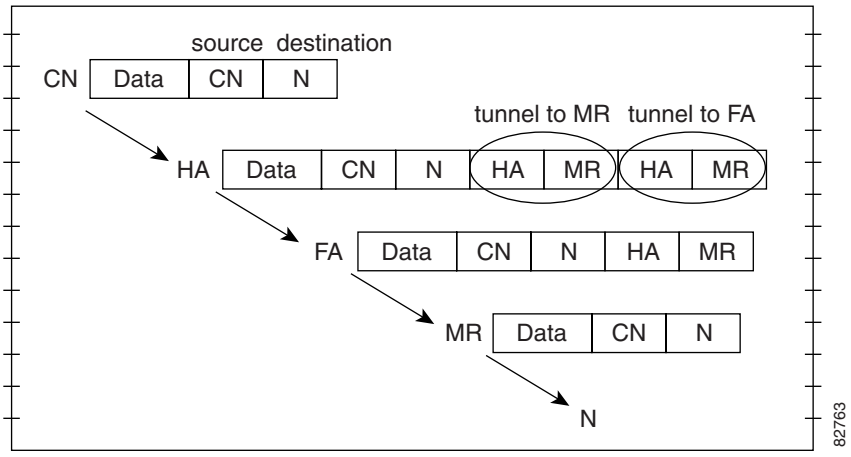
Registration

The home agent processes the registration request from a mobile access router the same way as a mobile node. The only difference is that an additional tunnel to the mobile access router is created and mobile networks are added to the routing table with next hop being the mobile access router. Packets to mobile networks are encapsulated twice.

How do packets reach devices on mobile networks?

On the home agent there are two tunnels. One tunnel is between the home agent and CoA. The other tunnel is between the home agent and the mobile access router. When a central office node sends a packet to a node on the mobile network, it arrives on the home agent.

The packet destined for mobile access router network is encapsulated with the home agent/mobile access router tunnel header, then encapsulated with the home agent/CoA tunnel header. The packet arrives on the foreign agent, which decapsulates the outer home agent/CoA tunnel header and forwards the packet to the mobile access router, which performs another decapsulation to deliver the packet to the destination.



HA = Home Agent
FA = Foreign Agent
CN = Central Node
N = Node
MR = Mobile Router

How are packets from devices on mobile networks routed?

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

In the case of a reverse tunnel, packets from devices arrive at the mobile access router, which encapsulates them before sending them to the foreign agent, which encapsulates the packets and sends them to the home agent. The home agent decapsulates packets and routes them to its networks.End User Interface

Static Network User Interface Commands

The mobile access router is a router that operates as a mobile node defined in Mobile IP specification, which allows a router to roam away from its home network and still provide connectivity for devices on its networks. For static network support, these mobile networks are locally attached to the router.

no ip mobile router Command

To enable the mobile access router and enter mobile access router configuration mode, use the **ip mobile router** command in global configuration mode. To disable the mobile access router, use the **no** form of this command.

The **address** subcommand configures the mobile access router home IP address and subnet mask. The address is used to register the mobile access router with the home agent. The address and subnet mask identifies home network and is used to discover when mobile access router is at home.

The **home-agent** subcommand tells the mobile access router which home agent to use during registration and detect when it is home. The **priority** level determines which is the home agent address to register with—although all addresses are on the same home agent. The home agent address list is used to detect when mobile access router is home; when the mobile access router receives an agent advertisement with IP source address on the list.

The **redundancy** subcommand provides fault tolerance by selecting one mobile access router in the group *name* to provide connectivity for the mobile networks. This is the active mobile access router. The passive mobile access routers wait until the active mobile access router fails before a previously passive mobile access router is changed to active mode. Only the active mobile access router registers and sets up the routing for the mobile networks. The redundancy state is either **active** or **passive**.

The **registration** subcommand controls the following mobile access router registration parameters:

- The **registration extend** command re-registers the mobile access router before the lifetime expires. The **expire** parameter is number of seconds to send registration request before expiration. The default is 120 seconds. The range is 1 to 3600. If no reply is received, mobile access router sends another registration request after the interval expires. The default is 10 seconds. The range is 1 to 3600. The mobile access router stops after the maximum number of retries are attempted. The default number of retries is 3. The range is 0 to 10. Zero means no retry.
- The **registration lifetime** command specifies the requested lifetime of each registration. The smallest value between the configured lifetime and the foreign agent advertised registration lifetime is used. The default is 65534 to ensure that the advertised lifetime is used, excluding infinite. The range is between 3 and 65535 seconds (which represents infinite). It is possible for the home agent to grant a lifetime that is shorter than the lifetime requested by the mobile access router.
- The **registration retransmit** command determines how to respond to retransmissions when no reply received and the mobile access router is not registered with the foreign agent. The **initial** parameter specifies how long to wait the first time before retrying when no reply is received. The default is 1000 milliseconds (1 second). The range is 10 to 10000 milliseconds (10 seconds). Each successive retransmission timeout period is double the previous period. This continues until the period reaches the the **maximum** value. The default is 5000 milliseconds (5 seconds). The range is 10 to 10000 milliseconds (10 seconds). Retransmission stops after the maximum number of retries attempted. The default **retry** is 3. the range is 0 to 10 retries. Zero means no retransmission.
- The **reverse-tunnel** subcommand enables reverse tunnel function. Only foreign agents that advertise reverse tunnel service, the mobile access router registers with a reverse tunnel request set. Once mobile access router is registered, it encapsulates packets from mobile networks using its tunnel to the home agent before sending packets to the foreign agent. The foreign agent sees packets sourced by mobile access router, and reverse tunnels them to home agent. This is necessary if the mobile networks are private addresses.

A mobile access router must be configured with a home address, subnet mask, home agent, and the mobility security association with the home agent. The mobility security association between home agent and mobile access router is defined by the **ip mobile secure host** and **ip mobile secure home-agent** parameters for home agent and mobile access router, respectively.

When mobile access router detects a foreign agent on a foreign network, it registers back to its home agent. The home agent authenticates the registration and binds the mobile access router to the foreign agent. In addition, home agent injects the mobile networks associated with the mobile access router into the routing table. These networks are reachable through the tunnel interface to mobile access router. When packets arrive at the home agent destined to the mobile networks, the home agent encapsulates them using the tunnel to the mobile access router, and encapsulates them again using the tunnel to the foreign agent. The foreign agent decapsulates the outer tunnel header and forward the packet to the mobile access router, which decapsulates tunnel header and forward original packet to destination.

The home agent must be configured with the **ip mobile host** *addr* **mobile-network** *name* and **ip mobile mobile-network** *name net mask* commands so the home agent can inject the networks into its routing table when mobile access router registers. This provides reachability and mobility for networks on the mobile access router.

For example, a mobile access router with an IP address of 10.1.1.10 is supported by a home agent for mobile network 10.1.1.0/24. When mobile access router registers back to its home agent, the home agent adds network 10.1.1.0/24 into the home agent routing table. The network can be summarized by routing protocols that redistribute Mobile IP routes.

The **show ip mobile registration** command displays the mobile access router registration table and the **show ip mobile router** command displays mobile access router information such as learned foreign agents, currently registered foreign agent, configured home agent, registration parameters, interface used for roaming, and so forth.

Mobile Router Configuration

```
ip mobile router
    address 10.1.1.10 255.255.255.0
    home-agent 10.1.1.20
    ip mobile secure home-agent 10.1.1.20 spi 100 key hex 12345678123456781234567812345678
```

Home Agent Configuration

```
ip mobile host 10.1.1.10 mobile-network MyJet virtual-network 10.0.0.0 255.0.0.0
ip mobile mobile-network MyJet 10.1.1.0 255.255.255.0
ip mobile secure host 10.1.1.10 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

show ip mobile router
show ip mobile mobile-network
ip mobile host

Basic Configuration Examples

Setting up a mobile access router consists of configuring the home agent and the mobile access router. The networks on the mobile access router, known as mobile networks, appears on the home agent while mobile access router roams around by using foreign agent

Home Agent Example Configuration

The home agent configuration consists of:

- Enabling Mobile IP
- Setting the mobile access router home network
- Setting the mobile access router IP address
- Setting the mobile networks on the mobile access router
- Setting the security association with mobile access router
- Setting the roaming interface

Enable Mobile IP by using the **router mobile** command.

Configure the home network by using the **ip mobile virtual-network** *home-net home-mask* command. This specifies that the home network is a virtual network, which means that the mobile access router is not physically attached to home agent.

Configure mobile access router by using the **ip mobile host** *address* **mobile-network** *network-tag* **virtual-network** *home-net home-mask* command. The IP address is in the home network.

Configure mobile networks on mobile access router by using the **ip mobile mobile-network** *network-tag net mask* command. The network may be individual subnets on interfaces of the mobile access router or summarized.

Configure security association with mobile access router by using the **ip mobile secure host** *address* **spi** *number* **key hex** *value* command. The SPI and key between home agent and mobile access router are known. The address is the mobile access router home IP address.

Verify the configuration by displaying mobile networks, mobile access router, and security association by using the following show commands:

- **show ip mobile** *mobile-network*
- **show ip mobile host** *address*
- **show ip mobile secure host** *address*

Foreign Agent Example Configuration

Setting the foreign agent configuration consists of:

- Enabling Mobile IP
- Enabling IRDP
- Enabling foreign agent service on an interface
- Setting a care-of address
- Enabling the visitor interface

Enable Mobile IP by using the **router mobile** command.

Enable IRDP advertisement as follows. This will send out periodic advertisements or only when solicitation received.

```
interface name
ip irdp
ip irdp max value
```

Enable foreign agent service on the interface by using the **ip mobile foreign-service** command. This appends the Mobile IP information, such as CoA, lifetime, service flags in the advertisement; as well as enabling foreign agent operation on interface.

Configure the care-of address by using the **ip mobile foreign-agent care-of** *interface* command. This is the foreign network termination point of the tunnel between the foreign agent and the home agent. The CoA is the interface IP address. The interface (physical or loopback interface) does not need to be the same as the visited interface.

Configure foreign agent service on an interface by using the following commands. For example, the maximum IRDP advertisement can be 10 seconds.

```
interface name
ip address address mask
ip mobile foreign-service
ip irdp
ip irdp max number
```

Verify configuration by displaying care-of address and interface with foreign agent service by using the following show commands:

show ip mobile global
show ip mobile interface

Maritime Configuration Example

A home agent provides routing for two mobile access routers Royal Caribbean and Carnival. Each mobile access router has a satellite link and wireless LAN link when docking. Each is allocated a network that can be partitioned further.

Setting the mobile access router configuration consists of:

- Enabling the mobile access router
- Setting the home IP address and home network mask
- Setting home agent IP address
- Setting security association with home agent
- Enabling a roaming interface

Enable mobile access router configuration submode, which enables the mobile access router, by using the **ip mobile router** command.

Configure mobile access router home IP address and home network mask by using the **address** *home-address mask* command. This address is same as what is configured on home agent for ip mobile host and ip mobile secure host.

Configure home agent IP address, which can be received by the home agent (physical or loopback interface, HSRP group address) by using the **home-agent** *address* command.

Configure security association with home agent by using the **ip mobile secure home-agent** *address* **spi** *number* **key hex** *value* command. The SPI and key between home agent and mobile access router are known. The address is the home agent IP address.

Configure roaming interface as follows. The IP address is an address on this subnet.

```
interface name
ip address address mask
ip mobile router-service
```

Verify configuration by displaying mobile access router information and security association.

show ip mobile router
show ip mobile secure home-agent *address*

Home Agent Configuration

```
router mobile
ip mobile virtual-network 10.1.0.0 255.255.0.0
ip mobile virtual-network 10.2.0.0 255.255.0.0
ip mobile host 10.1.0.1 mobile-network RoyalCaribbean virtual-network 10.1.0.0 255.255.0.0
ip mobile mobile-network RoyalCaribbean 10.1.0.0 255.255.0.0
ip mobile host 10.2.0.1 mobile-network Carnival virtual-network 10.2.0.0 255.255.0.0
ip mobile mobile-network Carnival 10.2.1.0 255.255.255.0
ip mobile mobile-network Carnival 10.2.2.0 255.255.255.0
ip mobile secure host 10.1.0.1 spi 101 key hex 12345678123456781234567812345678
ip mobile secure host 10.2.0.1 spi 102 key hex 23456781234567812345678123456781
!
interface Loopback 0
ip address 1.1.1.1 255.255.255.255
```

Foreign Agent Configuration

```
router mobile
ip mobile foreign-agent care-of serial0
!
interface serial0
ip irdp
ip irdp maxadvertinterval 0
ip mobile foreign-service
```

Royal Caribbean Mobile Router Configuration

```
interface loopback0
ip address 10.1.0.1 255.255.255.255
router mobile
ip mobile router
address 10.1.0.1 255.255.0.0
home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 101 key hex 12345678123456781234567812345678
!
interface serial 0
ip mobile router-service roam
ip mobile router-service solicit
interface ethernet 0
ip mobile router-service roam
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
interface ethernet 2
ip address 10.1.2.1 255.255.255.0
```

Carnival Mobile Router Configuration

```
interface loopback0
ip address 10.2.0.1 255.255.255.255
router mobile
ip mobile router
address 10.2.0.1 255.255.0.0
home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781
!
interface serial 0
ip mobile router-service roam
ip mobile router-service solicit
interface ethernet 0
ip mobile router-service roam
interface ethernet 1
ip address 10.2.1.1 255.255.255.0
interface ethernet 2
ip address 10.2.2.1 255.255.255.0
```

Dynamic Networks

A static network allowed mobile networks to roam by using static configurations on the home agent. When the mobile access router registered, the home agent would look up the configured mobile networks and add them to its routing table to be redistributed by using Interior Gateway Protocol (IGP). This scheme enforces mobile networks on a mobile access router, but it requires configuration for every mobile access router and is inflexible to network changes on the mobile access router.

A static network supports stub routers only. This allows mobile access router to roam, behaving like a mobile node. The difference is that the home agent treats this mobile node as a mobile access router. The home agent either advertises the mobile access router networks during configuration, when the mobile access router is at home, or when it is registered.

A dynamic network allows a mobile access router to register its mobile networks dynamically with the home agent, which advertises the mobile network as an attached network. When the network is enabled or disabled on the mobile access router, it registers with the home agent for notification purposes. The routing of packets to the devices on the networks is the same. The registration procedure is extended to include the network, prefix, and state information.

Since the new extensions support dynamic registrations of mobile networks, vendor-specific extensions (VSE) are used. Critical Vendor/Organization Specific Extension (CVSE) RFC 3115 is used, because it is mandatory that the home agent be able to process these extensions. Otherwise, home agent rejects the registration requests.

Mobile Access Router Operation

The mobile access router is configured to register with mobile networks, and when the mobile access router registers with the home agent, it appends a CVSE containing the configured mobile networks. For reregistration, a mobile access router does not append a CVSE. If mobile network is deconfigured while registered, the mobile access router sends a registration with a CVSE for network deletion.

If a mobile network is configured while registered, mobile access router sends a registration with a CVSE to add a network. Support routes using mobile access router interfaces are configured for mobile network.

Home Agent Operation

The home agent is configured to accept mobile access router registration requests containing mobile networks CVSE. The home agent processes the CVSE and adds or deletes routes to the mobile networks through the mobile access router. If a route already exists, the home agent ignores the addition of the network. The home agent deletes routes when notification of a network deletion is received.

Foreign Agent Operation

Although there is no mobile access router specific operation needed, there is a need to support the new CVSE. The foreign agent needs to understand the CVSE to be able to parse the extensions in the registration request to relay to the home agent.

Bandwidth usage between a foreign agent and the mobile access router can be reduced if the foreign agent is configured to strip off the home agent-mobile router tunnel header and then forward the original packet to the mobile access router. By recognizing the CVSE in the request, the foreign agent identify the destination as a mobile access router with mobile networks, and the foreign agent will forward packets from the home agent destined for the registered mobile networks directly to the mobile access router.

Make sure that dynamic network support interoperates with static network support, even for the same mobile access router. This feature is integrated in the existing Mobile IP subsystems, which are in the PLUS (-s-) images.

Related Commands

ip mobile mobile-networks name register

The **ip mobile router mobile-network register** command specifies that mobile networks can be dynamically registered on a home agent by a mobile access router. This command is used in conjunction with the **mobile-network** command. When the mobile access router registers with mobile networks, the home agent looks up the mobile network configuration and verifies that **register** is configured before adding routing entries to the mobile networks. If the mobile access router is not configured properly, the home agent rejects the request with error code 129, administratively prohibited. It is possible for *name* to have both statically configured mobile networks and dynamically registered mobile networks. For example:

```
router mobile
ip mobile home-agent
ip mobile host 100.0.0.1 interface Ethernet 1
ip mobile mobile-networks 100.0.0.1
  register
ip mobile secure host 100.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

ip mobile router mobile-network interface

The **ip mobile router mobile-network interface** command specifies which interface is connected to the mobile network on the mobile access router. The interface IP network number and mask are added to the registration request that notifies the home agent. Once the home agent acknowledges the mobile network, mobile access router no longer adds the mobile network information to the requests. For example:

```
router mobile
ip mobile router
 address 100.0.0.1 255.0.0.0
 home-agent 100.0.0.3
 mobile-network Ethernet3/2
 register lifetime 120
```

show ip mobile binding

When the **show ip mobile binding** command is entered, the registered mobile networks are also displayed on the home agent. For example:

```
Router#show ip mobile binding
Mobility Binding List:
Total 1
100.0.0.1:
    Care-of Addr 30.0.0.2, Src Addr 30.0.0.2
    Lifetime granted 00:02:00 (120), remaining 00:01:23
    Flags sbdmgvt, Identification BE8038D7.D2E15D80
    Tunnel0 src 100.0.0.3 dest 30.0.0.2 reverse-allowed
    MR Tunnel1 src 100.0.0.3 dest 100.0.0.1 reverse-allowed
        MR mobile-network 100.0.0.1
        Registered Mobile Networks 20.0.0.0/255.0.0.0 <--- NEW
        Routing Options -
```

debug ip mobile host

When a **debug ip mobile host** command is configured and a mobile network is dynamically registered on the home agent, the following messages are displayed:

```
MobileIP: HA 126 received registration for MN 100.0.0.1 on Ethernet3/2 using COA 30.0.0.2
HA 1\
00.0.0.3 lifetime 120 options sbdmgvt
MobileIP: MN 100.0.0.1 - authenticating MN 100.0.0.1 using SPI 100
MobileIP: MN 100.0.0.1 - authenticated MN 100.0.0.1 using SPI 100
MobileIP: Mobility binding for MN 100.0.0.1 created
MobileIP: Roam timer started for MN 100.0.0.1, lifetime 120
MobileIP: MN 100.0.0.1 is now roaming
MobileIP: Gratuitous ARPs sent for MN 100.0.0.1 MAC 00d0.ff79.5c55
00:05:41:
MobileIP: Insert host route for 100.0.0.1/255.255.255.255 via gateway 30.0.0.2 on Tunnel0
MobileIP: Add mobnet for MR 100.0.0.1 20.0.0.0/255.0.0.0 <- NEW
00:05:41:
MobileIP: Insert host route for 20.0.0.0/255.0.0.0 via gateway 100.0.0.1 on Tunnel1
00:05:41:
MobileIP: HA accepts registration from MN 100.0.0.1
MobileIP: MN 100.0.0.1 - MH auth ext added (SPI 100) to MN 100.0.0.1
MobileIP: MN 100.0.0.1 - HA sent reply to 30.0.0.2
```

show ip mobile router

When the **show ip mobile router** command is entered, mobile networks that have been configured and associated with mobile access router interfaces, are displayed on the mobile access router. The pending message is shown next to the mobile network while the mobile access router attempts to register the network. Once home agent accepts the registration, the pending message disappears. For example:

```
Router#show ip mobile router

Mobile Router
    Enabled 04/10/01 21:06:12

Configuration:
    Home Address 100.0.0.1 Mask 255.0.0.0
    Home Agent 100.0.0.3 Priority 100 (best)
    Registration lifetime 120 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 120, Retry 3, Interval 10
    Mobile Network Ethernet3/2 (20.0.0.0/255.0.0.0) <- NEW

Monitor:
    Status -Registered-
    Active foreign agent 20.0.0.2, Care-of 30.0.0.2
    On interface Ethernet3/1
    Tunnel0
```

show ip mobile router registration

The **show ip mobile router registration** command is entered, extensions in the registration request are displayed on the mobile access router. The **Add** or **Delete** message appears after the **Mobile Network** extension to specify action requested in last registration from mobile access router. For example:

```
Router#show ip mobile router registration

Mobile Router Registrations:
```

```
Foreign agent 20.0.0.2:
    Registration accepted 04/12/01 08:48:07, On Ethernet3/1
    Care-of addr 30.0.0.2, HA addr 100.0.0.3, Home addr 100.0.0.1
    Lifetime requested 00:02:00 (120), Granted 00:02:00 (120)
    Remaining 00:01:36
    Flags sbdmgvt, Identification BE805B64.AFE88540
    Register next time 00:00:36
    Extensions:                                  <- NEW
        Mobile Network Add 20.0.0.0/8            <- NEW
        MN-HA Authentication SPI 100             <- NEW
```

debug ip mobile router detail

When the **debug ip mobile router detail** command is configured and the mobile network is registered on the mobile access router, the following messages is displayed:

```
1d09h: MobRtr: New agent 20.0.0.2 coa 30.0.0.2 int Ethernet3/1 MAC 00b0.8e35.a055
1d09h: MobRtr: Register reason: left home
1d09h: MobRtrX: Extsize 18 add 1 delete 0 <- NEW
1d09h: MobRtrX: Add network 20.0.0.0/8            <- NEW
MobileIP: MH auth ext added (SPI 100) to HA 100.0.0.3
1d09h: MobRtr: Register to fa 20.0.0.2 coa 30.0.0.2 home 100.0.0.1 ha 100.0.0.3 life 120
int Ethernet3/1 flag sbdmgvt cnt 0 id BE804340.447F50A4
1d09h: MobRtr: Status Isolated -> Pending
1d09h: MobRtr: MN rcv accept (0) reply on Ethernet3/1 from 20.0.0.2 lifetime 120
MobileIP: MN 100.0.0.3 - authenticating HA 100.0.0.3 using SPI 100
MobileIP: MN 100.0.0.3 - authenticated HA 100.0.0.3 using SPI 100
1d09h: MobRtr: Status Pending -> Registered
1d09h: MobRtr: Add default gateway 20.0.0.2 (Ethernet3/1)
1d09h: MobRtr: Add default route via 20.0.0.2 (Ethernet3/1)
```

Configuration Example

The configuration is similar to static network support. For example:

Home Agent

```
router mobile
ip mobile home-agent
ip mobile host 100.0.0.1 interface Ethernet3/1
ip mobile mobile-networks 100.0.0.1
  register                        <--- NEW
ip mobile secure host 100.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

Mobile Router

```
router mobile
ip mobile router
 address 100.0.0.1 255.0.0.0
 home-agent 100.0.0.3
 mobile-network Ethernet3/2 <- NEW
 register lifetime 120
```

Static and Dynamic Collocated Care-of Address

A collocated care-of address (CCoA) terminates the tunnel from a home agent to a mobile device. This is in contrast to a care-of address (CoA), where a foreign agent is registered to a home agent, and the mobile device registers with the foreign agent. This allows the mobile device to roam to foreign networks where foreign agents are not deployed or where foreign agents are present, but foreign agent functionality is not available.

On the mobile access router, the IP address of the interface configured for roaming is also the CCoA address. This address can be a fixed IP address (Static CCoA), or it can be dynamically acquired (Dynamic CCoA) by using Point-to-Point Protocol (PPP)/IP Control Protocol (IPCP) or DHCP.

A Static CCoA is used where the mobile access router roaming interface IP address remains fixed, for example in Cellular Digital Packet Data (CDPD) wireless network. A Dynamic CCoA is used where the interface is configured to acquire its IP address by using DHCP and it is in **no shut** mode.

When mobile access router roams into a foreign network, first attempts to discover foreign agents. If the mobile access router discovers a foreign agent, the mobile access router with CoA configured attempts to register with the foreign agent. It sends a registration request (using an advertised CoA) to a foreign agent. The foreign agent relays the request to the home agent. The home agent process it and sends a reply to the foreign agent. The foreign agent relays the reply to mobile access router. The routing path between the home agent and the foreign agent (CoA) is set up after successful registration.

If it does not find a foreign agent, a mobile access router gets an address in the foreign network and sends a registration request directly to the home agent, using the address assigned to the mobile access router by the foreign network as the CCoA. The home agent process the request and sends a reply to the mobile access router. The routing path between the home agent and the mobile access router CCoA interface is set up after successful registration.

When the mobile access router detects that it is at home, it sends a deregistration request to its home agent.

The following events trigger a registration:

- A foreign agent advertisement is received, and the mobile access router has a reason to register.
- An active foreign agent advertisement (IRDP lifetime) expired, and the mobile access router chooses to register with another foreign agent.
- The registration timer expired due to the retransmission or lifetime aging.
- Recovery from the home agent that replied with a denial of service due to a mismatched ID.
- Recovery from a foreign agent, that replied with a denial of service as the result of a lower lifetime.
- After configuration (if the mobile access router has been configured for roaming and has a reason to register with a foreign agent).

A mobile access router might register with a foreign agent or a home agent for the following reasons:

- Movement is detected.
- A foreign agent reboot is detected.
- The mobile access router is isolated.
- A better interface on a reliable foreign agent is discovered.
- The mobile access router roams to on foreign network without an active foreign agent.
- The mobile access router roams on its home network when it has active foreign agent.

When a registration reply is received, the mobile access router processes it as if the reply message address equals the mobile access router interface IP address. The mobile access router finds the request in the registration table that corresponds to the reply. It authenticates the reply and sets a routing path between the mobile access router and the home agent. Also, it creates a default route through the foreign network.

Enabling CCoA

The **ip mobile router-service collocated** command configures the interface for CCoA. The interface must first be configured as a roaming interface by using the **ip mobile router-service roam** command; otherwise, an error message is displayed.

If the mobile access router is unable to register, it waits a default number of seconds and tries again. The default wait time is 60 seconds, can be configured by using an interface configuration command.

Default Gateway

If you change from a static IP address to DHCP address acquisition on a roaming interface, the static gateway address is not needed for CCoA. Instead, a default router address is obtained from DHCP when the IP address is acquired and the default router address is used as the CCoA gateway address. The gateway address is reset to 0.0.0.0 and the *gateway* keyword is no longer available on the CCoA command line.

When the interface acquires an IP address, the DHCP default router address is used as the CCoA gateway. In the opposite case, if a DHCP address configuration is changed from a DHCP-acquired IP address to a static IP address, the CCoA gateway address is set to 0.0.0.0 and you are warned that no CCoA default gateway is configured.

When a mobile access router is configured with a static IP address, the default gateway must be provided in the configuration by using the **ip mobile router-service collocated** command. This gateway address must be on the same network as the interface configured for static CCoA. The mobile access router uses this address as the next hop destination for Mobile IP Registration Request (RRQ)s, Upon receiving a successful Mobile IP Registration Reply (RRP), the mobile access router uses this address for the mobile access router default route and gateway.

CCoA Registration

When registering with its CCoA, the mobile access router sets decapsulation by the mobile node in the RRQ and uses the CCoA as the RRQ source address. The RRQ requests Generic Routing Encapsulation (GRE) tunneling if configured to do so. The RRQ is sent directly to the home agent. If, after the initial registration retries, the mobile access router has not successfully registered, it waits a set number of seconds and tries again. The default wait time is 60 seconds and can be configured by using the **ip mobile router-service collocated registration retry** interface command.

When the router is booted or when it is configured for roaming, an interface configured for dynamic CCoA attempts to find foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile access router registers with the advertised CoA. If a foreign agent is not found, the mobile access router registers with the CCoA.

A roaming interface that has discovered (and possibly registered with) a foreign agent can be made to immediately register a static or dynamic CCoA by using the **ip mobile router-serv collocated ccoa-only** command.

The foreign agent registration remains if you configure the interface by using the **ip mobile router-serv collocated** command. This command permits a roaming interface to discover foreign agents when the interface first comes up. If foreign agents are discovered, CCoA registration remains disabled unless the **ip mobile router-serv collocated ccoa-only** command is invoked. If a foreign agent is not discovered, CCoA registration is automatically enabled.

An interface configured for both foreign agent CoA and CCoA registration always prefers foreign agent CoA registration. When foreign agent advertisements are heard, the interface registers the foreign agent CoA, even if it has registered a CCoA. Otherwise, when a CCoA is present or acquired, it is registered.

To facilitate faster roaming, the interface registers a foreign agent CoA when an advertisement is heard or it registers a CCoA when an address is acquired, depending on which event occurs first. (Previously, the router waited to hear several advertisements before registering a foreign agent CoA.)

When a DHCP interface is **no shut**, or when an interface that is **up** is first configured for DHCP, DHCP IP address acquisition (discovery) begins. Address discovery attempts are repeated at increasingly longer intervals (up to 60 seconds) until an address is acquired. During discovery the interface is IP-enabled, so IP packets can be processed in support of IRDP and MIP registration even though the interface has no IP address.

A roaming interface configured for foreign agent CoA support sends solicits immediately and, if an advertisement is heard, the interface registers a CoA through the foreign agent. If the interface is also configured for CCoA registration and no advertisements have been heard, DHCP triggers CCoA registration. If the interface is configured **ccoa-only** (ignoring foreign agents, if any) no solicits are sent when the interface comes up. When an IP address is acquired, the interface attempts to register the newly acquired CCoA.

Even if the interface registries through a foreign agent, an IP address can be acquired through DHCP, though it does not affect the foreign agent registration. A foreign agent-registered interface retains the acquired IP address, to be used for a subsequent CCoA registration.

When a linkUp trap is received on a DHCP roaming interface, one or more attempts are made to renew the current IP address. If the attempts fail, the interface attempts to acquire a new DHCP address. This is done by invoking the renew/release/discover function.

When a CCoA-registered interface ends its registration in response to a linkDown trap event, the CCoA registration retry timer is started. If no linkUp event occurs before the timer expires, the interface makes one or more attempts to renew its current DHCP IP address or it attempts to acquire a new IP address. This is also done by invoking the renew function.

Foreign-Agent Discovery

Unless configured for **ccoa-only**, a roaming interface with static IP address or DHCP address begins soliciting as soon as the interface comes up. If it has a DHCP address, solicts can be sent and advertisements heard even without an IP address having been acquired. If the interface acquired its IP address by using IPCP, the interface must acquire an IP address before it can solicit.

To support CCoA, a default gateway address is required. This address is used as the default gateway for CCoA registrations and as a default route after the interface is registered. For Static CCoA on an Ethernet interface, a default gateway address must be provided through the roaming interface CCoA configuration. For DHCP interfaces, DCCOA registration use the DHCP default router address and, once the interface is registered, the address is also used for the mobile access router default route and gateway.

When a roaming interface is configured to acquire an IP address by using PPP/IPCP and it is in no shut mode, address negotiations with a peer begin. After the interface acquires an IP address, it attempts to solicit foreign agents or to register the acquired IP address as the CCoA.

If the solicit messages end and no foreign agent advertisements have been heard, further solicit messages are disabled and advertisements from foreign agents are ignored. Advertisements from home agents are still processed to determine whether the mobile access router has returned home. Disabling CCoA again enables solicit and foreign agent advertisement processing.

CCoA Tunneling

When registered using a CCoA, the mobile access router CCoA becomes the endpoint of a tunnel from the home agent. The mobile access router de-encapsulates the packet from the home agent sent through the tunnel to the CCoA.

This home agent-to-CCoA tunnel is in addition to the home agent-to-mobile access router home address tunnel that is created on the mobile access router when registering with mobile networks. To avoid the use of two tunnels and the resulting double encapsulation, the mobile access router optimizes tunneling by creating only one of the tunnels. On the home agent side, only the home agent-to-CCoA tunnel is certain to be created, because the home agent-to-mobile access router tunnel is not created until a mobile access router's mobile networks are added to the routing table, so tunnel optimization uses only the home agent-to-CCoA tunnel.

The single home agent-to-CCoA tunnel created during registration is used to reverse tunnel packets to the home agent, if the mobile access router is configured for reverse tunneling.

Mobile Access Router Configured as a Foreign-Agent

A mobile access router might also be configured as a foreign agent. If the mobile access router is configured as a foreign agent using the CCoA as the foreign agent CoA, the mobile access router sends an agent advertisement when that CCoA changes. An advertisement is sent even if the mobile access router is not configured for periodic advertisements to notify mobile nodes on attached networks to register using the new CoA.

Movement Detection and Layer 2 Signaling

Previously, only interface up/down signals or interface IP address changes on the roaming interface could trigger mobile access router CCoA roam processing. But some roaming scenarios require other internal or external signaling to detect movement and perform timely hand-offs. For example, an Ethernet interface connected to a WLAN through an 802.11 bridge. The wireless link might go up or down, but without some kind of signalling, a mobile access router Ethernet interface is not aware of the change. A mobile access router foreign agent CoA interface must wait until the foreign agent advertisement holdtime expires. In a CCoA-only scenario, the mobile access router would receive no indication that the status of the interface is changed.

The Wireless Mobile Interface Card (WMIC) connects to the mobile access router thought the Fast Ethernet interfaces. The 802.11 Layer 2 transitions (associations and disassociations) that take place on the WMIC are signaled by using SNMP messaging, specifically the Interface MIB linkUp and linkDown traps are sent to the mobile access router Ethernet or VLAN interface.

Mobile Access Router SNMP Message Processing

The mobile access router interface must be configured for roaming (foreign agent CoA registration by default) and if desired, CCoA registration. The mobile access router must also be configured to receive SNMP trap messages. The SNMP process receives the traps and invokes a registry permitting the mobile access router to examine the trap information. The mobile access router determines:

- If the trap was received on a roaming interface
- If the trap is a linkUp or linkDown event, ignoring others
- If the trap is from the Dot11Radio0 interface
- If this is a linkDown trap, examine the locIfReason information, processing only **down** or **administratively down** traps

DHCP and mobile access router processing occurs each time a valid linkUp trap or linkDown trap is received, even if the previous trap received was also linkUp. The mobile access router keeps no history of traps.

linkUp Trap Processing

When a linkUp trap event occurs, the DHCP client must either renew the current IP address or acquire a new IP address as quickly as possible. If a DHCP interface is without an IP address, address acquisition (Discover) is started.

The **ip dhcp client mobile renew count <***num***> interval <***msec***>** command permits you to configure the number of renew attempts and the interval between attempts when DHCP Renew is invoked. The configured values override any values passed by the DHCP Renew caller.

If IP address Discovery has started and it is between attempts (waiting for the next retry), address discovery immediately begins again.

If the interface already has a DHCP-acquired IP address, the mobile access router does not know if it is on the same subnet as before, so the mobile access router attempts to renew the current address. This reduces DHCP messaging if the mobile access router is reassociated to the same subnet. If a DHCP NACK message is received from a DHCP server on another subnet, or no DHCP ACK is received, the interface releases the current IP address and uses Discover to acquire a new IP address.

When a linkUp trap is received on a roaming interface, the event is handled as if the roaming interface just came up. For example, solicits are sent if appropriate and the mobile access router determines if this interface, compared to other roaming interfaces, should register. Dynamic address acquisition can trigger DCCoA registration.

Subsequent linkUp traps are processed the same way. However, if the interface is already registered, and nothing else has changed that affects the registration decision, the router does not attempt a new registration.

linkDown Trap Processing

The interface keeps any DHCP-acquired IP address. Receipt of a valid linkDown trap starts a reassociation hold-down timer. This timer is configurable timer with a range of 0-5000 ms. The default is 1000 ms.

This hold-down period delays the response to the trap, typically an attempt to register using the next best mobile access router interface, until the WMIC bridge has had time to reassociate on a new subnet. The timer value should reflect the worst case time expected to reassociate in a particular environment. The mobile access router remains registered during this hold-down period and foreign agent data is retained.

If a linkUp trap arrives before the hold-down timer expires, the mobile access router remains registered and foreign agent data is retained. Solicits are sent to find foreign agents and the DHCP IP address renewal and discovery process begins.

If the hold-down timer expires or the hold-down delay was 0, mobile access router processing proceeds as if the interface just went down. Any foreign agents heard on this interface are deleted from the foreign agent list and, if registered on the interface, the mobile access router deletes the current registration and tries to register by using the next best roaming interface. Solicits are sent to find foreign agents and the DHCP IP address renewal begins.

If a linkUp trap does not arrive after a linkDown event has been processed, the mobile access router may register by using a another lower priority interface. Even without a linkUp trap, a foreign agent advertisement triggers foreign agent registration again and DHCP address acquisition triggers a CCoA registration.

Example Configurations

This section provides CCoA and DHCP configuration examples.

SNMP Trap Configuration Example

SNMP linkup trap and linkdown trap are used for Layer 2 signaling on a roaming interface in DCCoA environment. Whenever the WMIC is associates or disassociates, a SNMP trap is sent to the router and the DCCoA roaming interface is notified.

WMIC

```
arp 85.85.85.1 000b.4681.0d40 ARPA BVI1
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 85.85.85.1 version 2c l2sig
```

Note 85.85.85.1 is the loopback IP address of the router. 000b.4681.0d40 is the MAC address of the F0/0 interface on the router (assuming that the WMIC F0 interface is connect to router F0/0 interface).

Mobile Access Router

```
    snmp-server manager
!
```

CCoA Configuration Example

The following is an example of the mobile access router configuration for CCoA:

Static CCoA

```
interface Serial1/0
    ip address 11.0.0.1 255.255.255.0
    ip mobile router-service roam
    ip mobile router-service collocated
```

Dynamic CCoA using PPP/IPCP

```
interface Serial2/0
    ip address negotiated
    encapsulation ppp
    ip mobile router-service roam
    ip mobile router-service collocated
```

Mobile Access Router

```
ip mobile secure home-agent 43.0.0.3 spi 100 key hex 11223344556677881122334455667788
ip mobile router
    address 20.0.4.1 255.255.255.0
    home-agent 43.0.0.3
```

Workgroup Bridge Example Configuration

The following example show a workgroup bridge configured to use SNMPv2 link traps:

Workgroup Bridge (WMIC)

```
arp 85.85.85.1 0000.abcd.1111 ARPA BVI1
snmp-server trap-source Dot11Radio0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 85.85.85.1 version 2c l2sig
```

Mobile Access Router

```
interface Loopback0
ip address 85.85.85.1 255.255.0.0
!
snmp-server community public RO
snmp-server enable traps ttyy
```

The following example shows a DHCP and SNMPv3 configuration example for DCCoA.

Mobile Access Router

```
interface FastEthernet0
    ip dhcp client mobile renew count 3 interval 20
    ip address dhcp
    ip mobile router-service roam
    ip mobile router-service collocated
    ip mobile router-service hold-down reassociate 2000
!
! Receive v1 or v2 traps
snmp-server community public RO
snmp-server enable traps tty
!

! Receive v3 traps
snmp-server engineID remote 85.85.85.3 1234
snmp-server user labusr labgrp remote 85.85.85.2 v3 auth md5 <SNMP user password on WGB>
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout 25
```

noauth Mode Example

The WMIC supports only SNMPv3 in **noauth** and **authNoPriv** modes.

The following example show a workgroup bridge configured for SNMPv3 link traps in **noauth** mode:

Workgroup Bridge

```
interface Loopback0
ip address 1.2.3.4 255.255.0.0
no ip route-cache

snmp-server group labgrp v3 noauth
snmp-server user labusr labgrp v3
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server host 1.7.35.35 version 3 noauth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4
snmp-server user labusr labgrp remote 1.2.3.4 v3
snmp-server group labgrp v3 noauth
snmp-server manager
snmp-server manager session-timeout <num>
```

noauth and authNoPriv Modes Example

The WMIC supports only SNMPv3 in **noauth** and **authNoPriv** modes.

The following example show a workgroup bridge configured for SNMPv3 link traps in **authNoPriv** mode:

Workgroup Bridge

```
interface Loopback0
ip address 1.2.3.4 255.255.0.0
no ip route-cache

snmp-server group labgrp v3 auth
snmp-server user labusr labgrp v3 auth md5 MD5passwd
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server host 1.7.35.35 version 3 auth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4
snmp-server user labusr labgrp remote 1.2.3.4 v3 auth md5 MD5passwd
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout <num>
```

Note For faster roaming during address acquisition, pings from the DHCP server to the client should be disabled.

Related Commands

This section describes the following related commands:

- ip mobile router-service collocated Command
- ip mobile router-service collocated registration retry Command
- ip mobile router-service hold-down Command
- ip dhcp client mobile renew
- debug snmp packet Command
- show ip mobile router Command
- show ip mobile router agent Command
- show ip mobile router interface Command
- show ip mobile router binding Command

ip mobile router-service collocated Command

The **ip mobile router-service collocated** command enables or disables CCoA processing on the interface. The interface primary IP address is used as the CCoA. The interface must already be configured as a roaming interface (**ip mobile router-service roam**); otherwise, an error message is displayed.

Use the **ip mobile router-service collocated** interface command to enable or disable CCoA processing on the interface.

ip mobile router-service collocated [gateway <*ipaddress*>] [**ccoa-only**]

where:

gateway <*ipaddress***>** is required for Ethernet interfaces with static IP addresses. The IP address specifies the default gateway to use when registering the CCoA on Ethernet. The default gateway IP address must be on the same link as the interface configured for static CCoA.

This address must not be 0.0.0.0 or 255.255.255.255 or the parameter will be rejected. Changing this gateway address while the mobile access router is registered triggers a new registration by using the new address.

When a roaming interface comes up the interface solicits foreign agent advertisements and if an advertisement is heard, it registers with a foreign agent CoA. If no advertisements are received, CCoA registration is enabled on the interface.

ccoa-only turns off agent discovery and the interface is immediately enabled for CCoA. Enabling CCoA by using this option on an interface already registered with a foreign agent CoA causes the mobile access router to immediately register with a CCoA.

Disabling CCoA by using the **no ip mobile router-service collocated** command on an interface already registered with a CCoA causes the interface to deregister its CCoA and begin foreign agent discovery.

If an Ethernet interface is configured with a static IP address, a gateway address must be configured. If the IP address configuration is changed acquire the IP address dynamically, the gateway address is the CCoA. The gateway address is reset to 0.0.0.0. If a configuration is changed to a static address, you are warned that CCoA processing will be disabled until CCoA is enabled with the specified gateway address.

The primary interface address is used as the CCoA, but registrations are rejected by the home agent if the CCoA and the home address are the same. So attempts to configure the addresses in this way trigger a warning message. Address checks are performed when interface IP addresses or CCoA gateway addresses are configured, or acquired dynamically, or when a home address is configured. If necessary, warnings are issued but **the configuration is still accepted**. At the time of registration, if the CCoA and home address are still the same, the mobile access router does not send the request and an error message is displayed.

ip mobile router-service collocated registration retry Command

CCoA interfaces use an interval timer to retry registration after a failed attempt.

Use the **ip mobile router-service collocated registration retry** interface command to set the interval for retrying CCoA registrations.

ip mobile router-service collocated registration retry <*1-65535*>

where *1-65565* is the number of seconds after a registration failure that the device waits before again attempting to register. The default value is **60** seconds.

The retry interval value is displayed by using the **show ip mobile router agent** command. If the interval timer is running, the time remaining until the next registration attempt is also displayed.

Note: Entering this command does not enable or disable CCoA support. It merely sets the timer interval.

ip mobile router-service hold-down Command

The **ip mobile router-service hold-down** [**foreign-agent** <*sec*> | **reassociate** <*msec*>] Layer 2 hold-down configuration command may be used to set reassociation delays for a roaming interface attached to a wireless link. For example:

```
(config-if)#ip mobile router-service hold-down [foreign-agent | reassociate]
```

foreign-agent	Time to wait before recognizing a new foreign agent (0-3600 seconds, default 0)
reassociate	Time to wait for layer 2 link reassociation (0 - 5000 msec, default 1000)

ip dhcp client mobile renew

The **ip dhcp client mobile renew** interface configuration command is for use on mobile DHCP clients. Clients automatically attempt to renew an existing IP address in response to certain events, for example, moving between wireless access points. The number of renewal attempts and the interval between those attempts, depending on network conditions, can be modified.

To set the number of IP address renewal attempts before starting the discover process, use the **ip dhcp client mobile renew count** command:

ip dhcp client mobile renew count <*count*> **interval** <*msec*>

count	Number of renewal attempts before starting discover. The range is 0–10 attempts. The default is 2 attempts.
interval	Interval (*msec*) between renewal attempts. The range is 1–1000 msecs. The default is 50 msecs.

debug snmp packet Command

The **debug snmp packet** command displays information about every Simple Network Management Protocol (SNMP) packet sent or received by the router, use the debug snmp packet command in privileged EXEC mode.

```
Router#debug snmp packet
```

The following is sample output from the debug snmp packet command. In this example, the messages the router receives display the following messages if SNMP trap is configured correctly.

WMIC

```
Router# debug snmp packet
Mar  1 00:04:40.508: SNMP: Queuing packet to 85.85.85.1
*Mar  1 00:04:40.509: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 28051
```

```
snmpTrapOID.0 = snmpTraps.3
ifEntry.1.5 = 5
ifEntry.2.5 = Virtual-Dot11Radio0
ifEntry.3.5 = 71
lifEntry.20.5 = administratively down
*Mar  1 00:04:40.515: SNMP: Queuing packet to 85.85.85.1
*Mar  1 00:04:40.515: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 28051
snmpTrapOID.0 = snmpTraps.3
ifEntry.1.1 = 1
ifEntry.2.1 = Dot11Radio0
ifEntry.3.1 = 71
lifEntry.20.1 = administratively down
*Mar  1 00:04:40.759: SNMP: Packet sent via UDP to 85.85.85.1
*Mar  1 00:04:41.009: SNMP: Packet sent via UDP to 85.85.85.1
```

Mobile Router

```
Router# debug snmp packet
*Mar  4 19:30:12.265: SNMP: Packet received via UDP from 40.20.0.12 on FastEthernet0/0
*Mar  4 19:30:12.513: SNMP: Packet received via UDP from 40.20.0.12 on FastEthernet0/0
```

show ip mobile router Command

The following is an example of the output from the **show ip mobile router** command when the interface is registered as DCCoA.

```
UUT1#sh ip mobile router

Mobile Router
   Enabled 03/01/02 02:44:14
   Last redundancy state transition NEVER

Configuration:
   Home Address 85.85.85.1 Mask 255.255.255.0
   Home Agent 30.10.0.2 Priority 100 (best) (current)
   Registration lifetime 60 sec
   Retransmit Init 1000, Max 5000 msec, Limit 3
   Extend Expire 120, Retry 3, Interval 10

Monitor:
   Status -Registered-
   Using collocated care-of address 40.20.0.11
   On interface FastEthernet0/0
   Tunnel0 mode IP/IP
```

The following is an example of the output from the **show ip mobile router** command when the interface is registered by using a CoA.

```
UUT1#sh ip mobile router

Mobile Router
   Enabled 03/01/02 02:44:14
   Last redundancy state transition NEVER

Configuration:
   Home Address 85.85.85.1 Mask 255.255.255.0
   Home Agent 30.10.0.2 Priority 100 (best) (current)
   Registration lifetime 60 sec
   Retransmit Init 1000, Max 5000 msec, Limit 3
   Extend Expire 120, Retry 3, Interval 10
```

```
Monitor:
   Status -Registered-
   Active foreign agent 40.20.0.2, Care-of 40.20.0.2
   On interface FastEthernet0/0
   Tunnel0 mode IP/IP
```

show ip mobile router agent Command

The following is an example of the output from the **show ip mobile router agent** command:

```
Router#show ip mobile router agent
Mobile Router Agents:
Foreign agent 45.0.0.2:
    Care-of address 42.0.0.2
    Interface Ethernet1, MAC 0030.9492.6627
    Agent advertisement seq 56649, Flags rbhFmGvt, Lifetime 36000
    IRDP advertisement lifetime 30, Remaining 29
    Last received 02/13/02 17:55:48
    First heard 02/13/02 11:21:46

Collocated Care-of address 11.0.0.1
    Interface Serial0/1
    Default gateway 11.0.0.2
    Registration retry interval 60
    Next CCoA reg attempt in 00:00:55 seconds
```

show ip mobile router interface Command

The **show ip mobile router interface** command output shows the Layer 2 link down hold-down value and the most recently processed link state trap.

```
mobrouter#show ip mobile router interface

Ethernet1:
    Priority 110, Bandwidth 10000, Address 55.0.0.8
    Periodic solicitation disabled, Interval 600 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Current 5000, Remaining 0 msec, Count 4
    Foreign agent hold down 0 sec
    Layer 2 reassociation hold down 5000 msec
    Last layer 2 link-state trap: linkDown
    Routing disallowed
    Collocated CoA 55.0.0.8 - Solicit FAs
```

show ip mobile router binding Command

The following is an example of the output from the **show ip mobile router binding** command on the home agent:

```
Router#show ip mobile binding
Mobility Binding List:
Total 1
20.0.4.1:
    Care-of Addr 12.0.0.1, Src Addr 12.0.0.1
    Lifetime granted 00:02:00 (120), remaining 00:01:54
    Flags sbDmgvt, Identification C05E97DB.167E8950
    Tunnel0 src 46.0.0.3 dest 12.0.0.1 reverse-allowed
    MR Tunnel0 src 46.0.0.3 dest 12.0.0.1 reverse-allowed
    MR mobile-network 20.0.4.1
    Routing Options - (D)Direct-to-MN
```

In the **Flags sbDmgvt** entry, the “D” indicates that the mobile node is registered using a CCoA. (A lower-case “d” indicates that the mobile node is registered using a foreign agent.)

CHAPTER 8

Foreign Agent Route Optimization

The Mobile IP v4 protocol does not allow direct routing from one mobile node to another mobile node or to a mobile network behind a mobile router. The protocol requires the traffic to go through the home agent, creating the problem of triangular routing.

Foreign Agent Route Optimization *injects* mobile network routes into a foreign agent routing table, enabling routing directly from one mobile network to another mobile network. This route optimization improves deployments that are running latency-sensitive applications.

Understanding Foreign Agent Route Optimization

After accepting a registration request from a mobile router with static and/or dynamic mobile networks, a home agent creates routing table entries for the mobile networks and advertises the reachability to these networks through the home agent–to–foreign agent and home agent–to–mobile router logical tunnel.

This network state is propagated to the network by using the Interior Gateway Protocol (IGP) and enables corresponding nodes to reach the mobile networks through the home agent. If Foreign Agent Route Optimization is not enabled, the traffic from corresponding nodes on networks directly connected to foreign agent interfaces are forced to take the path to the home agent. If Foreign Agent Route Optimization is enabled, traffic is passed from the directly connected interface to the mobile router.

Home Agent Processing of the Registration Request

After authenticating the user, if the home agent receives a Mobile IP registration request from any mobile router, the home agent looks up the configuration for all the static networks associated with that mobile router. It also learns the dynamic mobile networks associated with the mobile router from the Dynamic Network Extension in the registration request.

The home agent constructs the Static and Dynamic Mobile Network extensions and sends them back to the mobile router as part of the registration reply. These extensions are protected by the Mobile-Home authentication extension.

The home agent does not send the static or dynamic mobile networks in a deregistration request reply message. However, for backward compatibility, the home agent does include a Dynamic Mobile Network Extension with a single dynamic mobile network prefix.

Foreign Agent Considerations

A foreign agent learns the configured static mobile networks and the registered dynamic mobile networks that are linked to a mobile router by parsing the Dynamic Mobile Network and the Static Mobile Network Normal Vendor/Organization Specific Extensions (NVSEs) from the successful registration reply from the home agent. (It is mandatory to have a security association between the home agent and the foreign agent.) If the foreign agent receives a successful registration reply from the home agent and if that message has no Foreign-Home Authentication extension in it, the foreign agent skips the route injection step.

Foreign Agent Processing of the Registration Request

A foreign agent processes a registration request the same way for all devices. On receiving a registration reply from a home agent, the foreign agent checks for the following:

- Static and Dynamic Mobile Network Extensions
- Foreign-Home Authentication Extension
- Route injection enabled
- Registration lifetime

The foreign agent injects the routes into the routing table and redistributes the routes by using IGP. The injected routes are stored in the local data structure and associated with a visitor entry.

The foreign agent, upon receiving a deregistration message with a zero lifetime, removes the routes from the routing table and deletes them from the local data structures.

Upon receiving a reregistration message with a new lifetime, the foreign agent injects the routes into the local data structure and associates them with the visitor entry.

Configuring Foreign Agent Route Optimization

The configuration command described in this section has been added to the Mobile IP subsystem.

ip mobile foreign-agent inject-mobile-networks

Use the **ip mobile foreign-agent inject-mobile-networks** command to enable foreign agent route optimization for mobile networks at the foreign agent.

ip mobile foreign-agent inject-mobile-networks [**mobnetacl** <*ACL*>]

The no form of the command disables foreign agent optimization:

no ip mobile foreign-agent inject-mobile-networks, disables the feature.

Syntax Description

mobnetacl <*ACL*>	(Optional) **mobnetacl** specifies a simple named or numbered access control list for controlling the mobile networks for which the foreign agent can provide route optimization.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Examples The following is sample output for the **show ip mobile globals** command.

```
Router#show ip mobile globals
IP Mobility global information:
Home Agent is not enabled

Foreign Agent

    Pending registrations expire after 120 secs
    Care-of addresses advertised
    Mobile network route injection enabled
    Mobile network route redistribution disabled
    Mobile network route injection access list test
        FastEthernet0/0 (70.70.70.1) - up

1 interface providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
NAT UDP Tunneling support enabled
UDP Tunnel Keepalive 110
Forced UDP Tunneling disabled
```

Related Commands

Command	Description

Caveats

The following are Foreign Agent Route Optimization caveats:

- After mobile router registration, any static mobile network configuration changes on the home agent are not reflected in the foreign agent routing table. There is no home agent–foreign agent signaling the removal of the mobile network routes. The route is removed when the router is deregistered.
- Explicit clearing of the mobile router bindings at the home agent does not remove the mobile network routes at the foreign agent.

Example Configurations

This section shows a configuration example for the foreign agent.

Foreign Agent

```
hostname gridley
!
interface Ethernet2/0
 ip address 10.0.19.102 255.255.255.240
 no ip route-cache
 no ip mroute-cache
 duplex half
!
interface Ethernet2/1
 ip address 20.20.20.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
interface Ethernet2/2
 ip address 30.30.30.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 20
 ip irdp minadvertinterval 10
 ip irdp holdtime 60
 ip mobile foreign-service registration-required reverse-tunnel
 ip mobile registration-lifetime 65535
 no ip route-cache
 no ip mroute-cache
 duplex half
!
interface Ethernet2/3
 ip address 90.90.90.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
router ospf 100
 log-adjacency-changes
 redistribute mobile subnets
 network 10.10.10.0 0.0.0.255 area 0
 network 20.20.20.0 0.0.0.255 area 0
 network 30.30.30.0 0.0.0.255 area 0
 network 90.90.90.0 0.0.0.255 area 0
!
ip classless
no ip http server
!
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent reg-wait 120
ip mobile foreign-agent inject-mobile-networks mobnetacl mob-net-list
ip mobile secure home-agent 30.30.30.1 spi 1400 key ascii cisco algorithm md5 mode
prefix-suffix
!
ip access-list standard mobile-net-list
 permit any
!
end
```

Mobile IP Security

All registration messages between a mobile node and home agent are required to contain the Mobile-Home Authentication Extension (MHAE).

The integrity of the registration messages is protected by a shared 128-bit key between a mobile node and home agent. The keyed message digest algorithm 5 (MD5) in "prefix+suffix" mode is used to compute the authenticator value in the appended MHAE. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a mobile node and foreign agent and between a foreign agent and home agent, respectively.

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

The Cisco IOS software allows the mobility keys to be stored on an authentication, authorization, and accounting (AAA) server that can be accessed using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) protocols. You can restrict who is allowed to register by using registration filters.

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

AAA in the Mobile IP Environment

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

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

Configuring RADIUS in the Mobile IP Environment

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

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

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

Configuring TACACS+ in the Mobile IP Environment

Terminal Access Controller Access Control System Plus (TACACS+) is an authentication protocol that provides remote access authentication and related services, such as event logging. For detailed information about TACACS+ configuration options, refer to the "Configuring TACACS+" chapter in the *Cisco IOS Security Configuration Guide*.

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

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

Example of a AAA Server Configuration

In the following AAA server configuration, the home agent can use an AAA server for storing security associations. Mobile IP has been authorized using TACACS+ server to retrieve the security association information, which is used by the home agent to authenticate registrations. The **user** is the mobile node IP address. The syntax for the security association is spi#*num* = *string*, where *string* is the rest of the IP address. This format can be imported into a CiscoSecure server.

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

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

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

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

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

IPSec in the Mobile IP Environment

Security associations establish trust between two devices in a peer-to-peer relationship. There are two types of security association. The first is Internet Key Exchange (IKE), which provides negotiation, peer authentication, key management, and key exchange. IKE provides a secure communication channel between two devices that is used to negotiate an encryption algorithm, a hash algorithm, an authentication method, and any relevant group information.

The second type of security association is called IPsec security association (IPsec SA). IPsec SA is unidirectional, thus requiring that separate IPsec SAs be established in each direction to provide non-repudiation, data integrity, and payload confidentiality. Non-repudiation is often necessary to verify that a transaction has taken place, such as a financial exchange between parties. Data integrity verifies that packets are not altered in transit by a third party. Payload confidentiality is provided by encryption.

It might be necessary to protect certain traffic on the mobile network. This is accomplished by enabling IPSec between the mobile access router and an IPSec gateway located behind the home agent. Since an IPSec tunnel is established within the Mobile IP tunnel, IKE renegotiation is unnecessary as the mobile access router moves about. The result is secure, scalable mobile networks based on standards.

The IPSec encryption algorithm that runs between the mobile access router and the IPSec gateway can either be Triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Note that AES provides greater security than DES and is more efficient than 3DES.

IPSec Interoperability

IPsec sets up its peering between the egress interface of the encrypting router and any interface on the decrypting router. This relationship is hampered because the egress interface of a mobile access router changes based on available network connectivity. In addition, the egress interfaces might have non-routable IP addresses associated with them, which makes setting up an IPsec session impossible using the standard model.

To overcome the problems, all traffic must exit the same interface that will always be up and will always have a routable IP address. The method applied in this example is anchoring the IPsec session to the loopback interface on the mobile access router. The home address of the mobile access router should be configured on a loopback interface because loopback interfaces are software and are always up.

It is possible to forward traffic into a loopback interface. If the traffic is not destined for the IP address of the loopback, the traffic exits the interface and is looped back into the router. At this point, normal routing processes take delivery of the packet.

The only way to forward traffic out a loopback is with the **set interface** target of a **route map** command. Using the features of route maps and loopback interfaces, you can configure IPsec on a mobile access router. All traffic from the mobile network that needs to be encrypted is sent by a route map out the loopback and back in to the router for normal delivery. When the traffic exits the loopback interface, the crypto map is applied and traffic is encrypted as necessary. For traffic to the mobile access router, the ingress interface is the loopback interface that has the crypto map to decrypt any protected content.

In summary, the loopback interface is always up and not affected by the movement of the mobile access router (in which the interface or point of attachment changes dynamically). This provides the invariant endpoint of the IPSec connection. Thus, the IPSec connection is always *alive* in conjunction with mobility.

IPSec Gateway

The IPSec gateway might be any Cisco router with IPSec software and an IPSec-capable image that corresponds to the mobile access router. The IPSec gateway is not required to have the Mobile IP feature set, because it is not providing mobility service. Since this router is acting as an IPSec traffic aggregator, it is recommended that you install hardware accelerator modules in the connected device for better performance. Ideally, the IPSec gateway router is a Cisco 7200 Series router with an ISA/VPN Acceleration Module (VAM) card, or a Catalyst 6500 switch with an American Contractors Exchange (ACE) card.

Figure 9-1 IPSec Gateway Network Topology

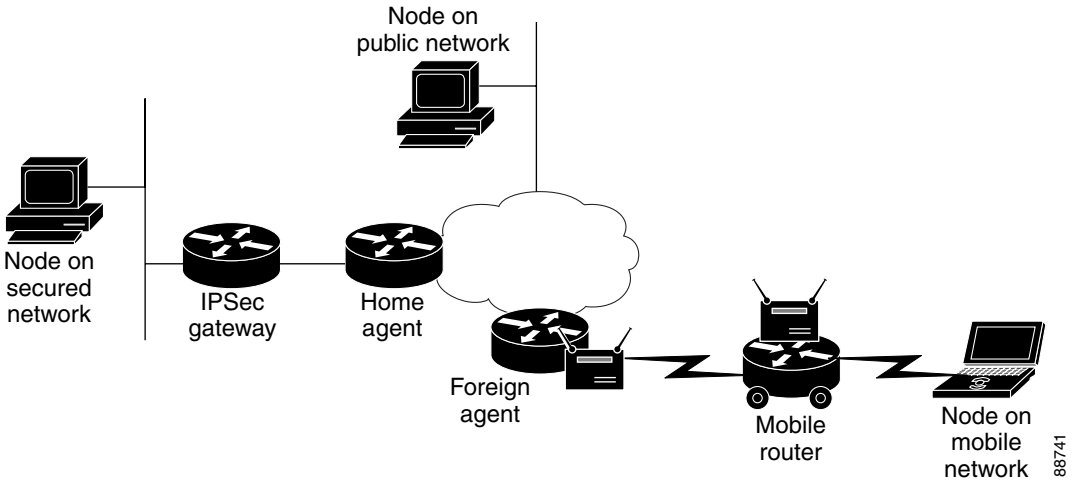
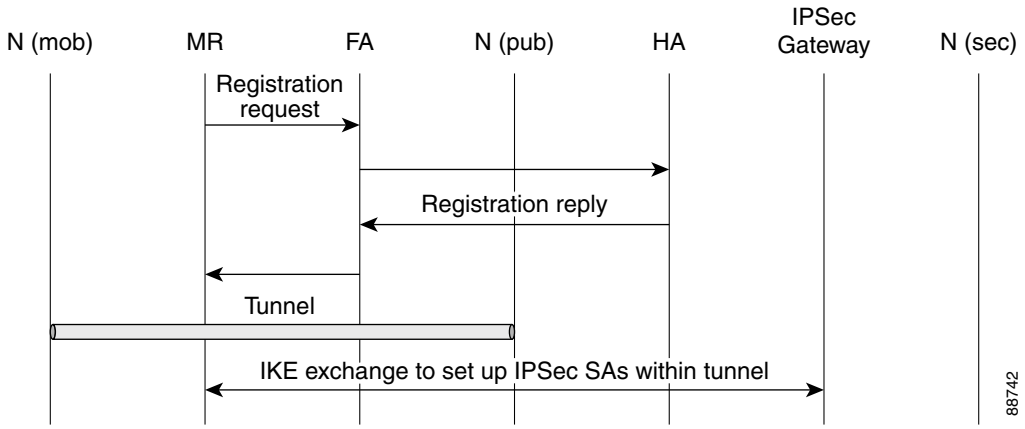


Figure 9-1 shows three types of nodes in the network topology: nodes on a mobile network, nodes on a secured network, and nodes on a public network. The mobile access router establishes an IPSec tunnel between it and the IPSec gateway to protect traffic to nodes on the secured network. Communications with nodes on the public network is not encrypted. The home agent and IPSec gateway must be deployed in the Demilitarized Zone (DMZ).

Figure 9-2 shows how a mobile access router sets up an IPSec tunnel with the IPSec gateway by exchanging IKE messages, which traverse the Mobile IP tunnel. The IPSec tunnel is established when traffic flows between a node on the secured network and a node on a mobile network.

Figure 9-2 IPSec Control Flow

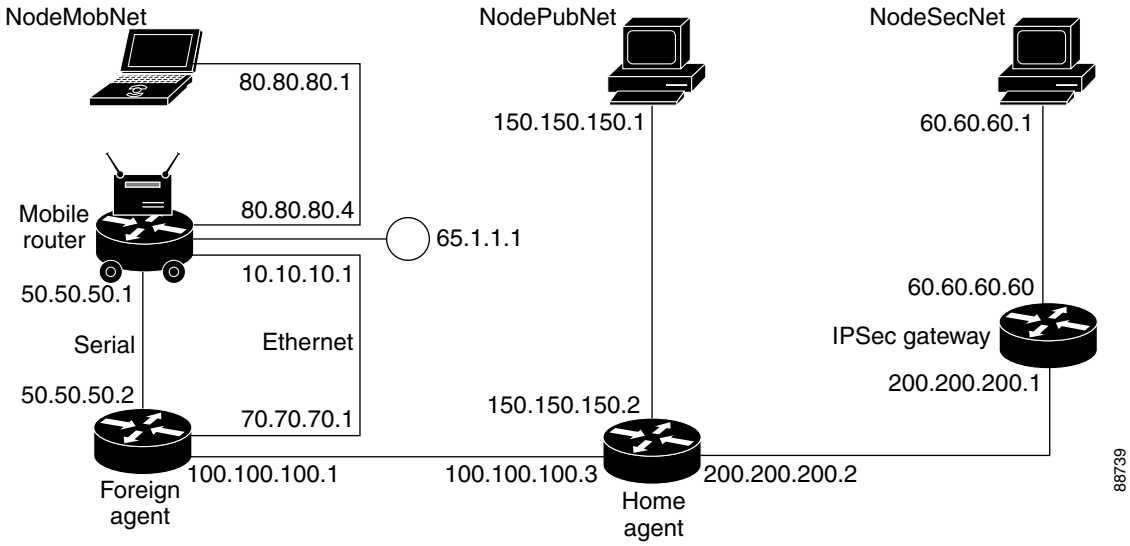


Data traffic can be categorized into either secure or public. Communications that must be protected are encrypted and wrapped in IPSec. Otherwise, packets are sent in the clear.

IPSec Configuration

This section contains configurations for the mobile access router, IPSec gateway, home agent, foreign agent, and mobile nodes in a specified network topology. Traffic is secured between the mobile access router network and networks in the home domain. The IPSec endpoints are the mobile access router and the IPSec Gateway located behind the home agent on the home network. The networks in the home domain in which protection is desired are placed behind the IPSec gateway.

Figure 9-3 IPSec Configuration Example



Example of IPSec Mobile Network Configuration

The mobile access router has one Ethernet interface on the mobile network and two interfaces, serial and Ethernet, connected to a foreign agent. The foreign agent is providing Mobile IP service only on the Ethernet interface, not on the serial interface.

The serial interface is a roaming interface with static collocated care-of-address. The roaming Ethernet interface is used to detect foreign agents. The other Ethernet interface is for the LAN on the mobile access router. All nodes on the mobile network use the mobile access router as the default gateway.

Note If the mobile access router has only one network interface, the mobile network and the roaming interface functions should be combined. If the mobile access router has multiple interfaces or VLANs, it should have a dedicated roaming interface and a mobile network interface.

The IPSec configuration must meet the following criteria:

- The mobile access router home address must be configured as a loopback address.
- The crypto map to encrypt traffic to the home network must be applied on the loopback interface (named *ToSecureNet* in the configuration example).
- The IPSec/IKE peer for the crypto configuration is the IPSec gateway IP address.
- On the inbound interface where the mobile access router networks are configured, a routemap must be applied to select the traffic to be encrypted (named *SecureNetPolicy* in the example configuration). This routemap sets the outbound interface to the loopback interface and forces crypto evaluation. This results in encryption if the traffic matches the crypto-map access control lists.
- The access control list must list the networks for which traffic must be encrypted. In the configuration example, the access control list is:

  ```
  access-list 155 permit ip 80.80.80.0 0.0.0.255 60.60.60.0 0.0.0.255
  ```

Since the source is 80.80.80.0/24, it corresponds to the mobile access router network connected on the Ethernet interface. The destination network is 60.60.60.0/24, which implies that all traffic towards 60.60.60.0/24 will be encrypted. Since communication with the network 60.60.60.0/24 is IPSec protected, this network is referred to as a *protected network*. All protected networks must be listed in the access control list. The last implicit entry in the access control list is *deny ip any any.* If the traffic does not match any of the previous entries and was not marked for encryption, the traffic is sent in clear.

Unprotected access is provided to all other (public) networks (those not listed the access control list with the permit clause). For example:

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 200.200.200.1
!
crypto isakmp peer address 200.200.200.1
!
crypto IPsec transform-set testtrans esp-des
!
!
crypto map ToSecureNet 10 IPsec-isakmp
 set peer 200.200.200.1
 set transform-set testtrans
 match address 155
!
```

```
interface Loopback1
 ip address 65.1.1.1 255.255.255.255
 crypto map ToSecureNet
!
interface Ethernet3/2
 ip address 10.10.10.1 255.255.255.0
 ip mobile router-service roam
!
interface Ethernet3/3
 ip address 80.80.80.4 255.255.255.0
 ip policy route-map SecureNetPolicy
!
interface Serial4/1
ip address 50.50.50.1 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 50.50.50.2
!
router mobile
!
ip local policy route-map SecureNetPolicy
!
ip mobile secure home-agent 100.100.100.3 spi 100 key hex 11223344556677881123344556677881 88
algorithm md5 mode prefix-suffix
ip mobile router
 address 65.1.1.1 255.0.0.0
 home-agent 100.100.100.3
 reverse-tunnel
!
access-list 155 permit ip 80.80.80.0 0.0.0.255 60.60.60.0 0.0.0.255
!
route-map SecureNetPolicy permit 10
 match ip address 155
 set interface Loopback1
```

Example of IPSec Gateway

The IPSec gateway IP address must be configured on a physical WAN interface of the mobile access router. Typically, this is the interface that receives traffic from and sends traffic to the home agent.

Home domain networks in which sensitive data requires encryption are located behind this gateway. Traffic between these networks and mobile access router networks is provided IPSec protection. The crypto map in sample configuration has the following access control list:

```
access-list 156 permit ip 60.60.60.0 0.0.0.255 80.80.80.0 0.0.0.255
```

This indicates that any traffic from protected network 60.60.60.0/24 that is going to mobile access router network 80.80.80.0/24 is selected for encryption and decryption. For example:

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 65.1.1.1
!
!
crypto IPsec transform-set testtrans esp-des
!
crypto map ToMobileNet 10 IPsec-isakmp
set peer 65.1.1.1
 set transform-set testtrans
 match address 156
!
interface Ethernet1/0/2
```

```
 ip address 200.200.200.1 255.255.255.0
 crypto map ToMobileNet
!
interface Ethernet1/0/3
 ip address 60.60.60.60 255.255.255.0
!
access-list 156 permit ip 60.60.60.0 0.0.0.255 80.80.80.0 0.0.0.255
```

Foreign Agent Example

To support mobile access router home domain network IPSec, no special configuration of the foreign agent is required. For example:

```
interface Serial1/2
 ip address 50.50.50.2 255.255.255.0
!
interface Ethernet3/1
 ip address 100.100.100.1 255.255.255.0
!
interface Ethernet3/3
 ip address 70.70.70.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 5
 ip irdp minadvertinterval 2
 ip irdp holdtime 15
 ip mobile foreign-service reverse-tunnel
!
router mobile
!
router rip
 redistribute mobile
 network 50.0.0.0
 network 70.0.0.0
 network 100.0.0.0
!
ip mobile foreign-agent care-of Ethernet3/1
```

Home Agent Example

Because the home agent does not participate in providing traffic protection, no special IPSec configuration is required at the home agent. The Mobile IP configurations are shown below:

```
interface Ethernet3/1
 ip address 100.100.100.3 255.255.255.0
!
interface Ethernet3/2
 ip address 200.200.200.2 255.255.255.0
!
interface Ethernet3/3
 ip address 150.150.150.2 255.255.255.0
!
router mobile
!
router rip
 redistribute mobile metric 1
 network 100.0.0.0
 network 150.150.150.0
 network 200.200.200.0
!
ip mobile home-agent
ip mobile virtual-network 65.0.0.0 255.0.0.0
ip mobile host 65.1.1.1 virtual-network 65.0.0.0 255.0.0.0
ip mobile mobile-networks 65.1.1.1
```

```
 description SecureTransport
 network 80.80.80.0 255.255.255.0
ip mobile secure host 65.1.1.1 spi 100 key hex 11223344556677881123344556677788 algorithm
md5 mode prefix-suffix
no ip mobile tunnel path-mtu-discovery
```

Node on Mobile Network Example

```
interface Ethernet3/3
 ip address 80.80.80.1 255.255.255.0
!
ip route 60.60.60.0 255.255.255.0 80.80.80.4
```

Node in Public Network Example

```
interface Ethernet1/1
 ip address 150.150.150.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 150.150.150.2
```

Node in Secure Network Example

```
interface Ethernet1/1
 ip address 60.60.60.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 60.60.60.60
```

Mobile Network Security Testing

From a node on the mobile network, you can ping a node in the protected network. You can ping from the protected network node to the mobile network node with same results. The first few packets might be dropped (due to ARP, IKE, or IPSec secure area setup). After the initial packet loss, ping should be successful.

IKE and IPSec security associations are established at mobile access router and IPSec Gateway. To see the IKE security association (SA) state, use the **show crypto** command. For example:

```
MobileRouter# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id        slot
       /        200.200.200.1   65.1.1.1         QM_IDLE       3              0
```

After the security area has been established, the state is typically QM_IDLE.

To see the IPSec secure area, use the **show crypto ipsec sa** command:

```
MobileRouter#show crypto ipsec sa
interface: Loopback1
    Crypto map tag: ToSecureNet, local addr. 65.1.1.1
protected vrf:
   local  ident (addr/mask/prot/port): (80.80.80.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0)
   current_peer: 200.200.200.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 397876, #pkts encrypt: 397876, #pkts digest 0
    #pkts decaps: 397559, #pkts decrypt: 397559, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
```

```
     local crypto endpt.: 65.1.1.1, remote crypto endpt.: 200.200.200.1
     path mtu 1514, media mtu 1514
     current outbound spi: 21E53ABF

     inbound esp sas:
<snip>
```

Notice the **#pkts encaps** and **#pkts decaps** counters. To clear the counters, use the **clear crypto sa counters** command.

Ping from a mobile access router node to a node on the secured network (or vice versa), and look at the value of counters again. The counters should match the number of ping packets you sent.

Other methods for detecting the encryption activity:

- Use the **debug ip packet detail dump** command, and observe that the contents do not appear to be logical.
- Attach a sniffer (or Pagent device) between the mobile access router and the IPSec Gateway, and watch the packets on the wire.
- Measure the size of packets as seen by egress interfaces on the mobile access router, home agent and IPSec gateway.

To clear the IKE security associations, use the **clear crypto isakmp** command:

```
MobileRouter#clear crypto isakmp <0-32766>
```

where *<0-32766>* is the connection ID of the secure area.

To clear the IPSec security associations, use the **clear crypto sa** command:

```
MobileRouter#clear crypto sa [counters | map | peer | spi | vrf]
```

where:

counters resets the secure area counters
map clears all secure areas for a given crypto map
peer clears all secure areas for a given crypto peer
spi clears secure areas by SPI
vrf clears VRF (Routing/Forwarding) instance

This command can also clear the packet counters, and it can be used for debugging.

IPSec Commands

encryption Command

Use the **encryption** command, a isakmp policy command, to establish IKE policy.

```
encryption {aes | aes 192 | aes 256}

Where:
aes specifies 128-bit AES
aes 192 specifies 192-bit AES
aes 256 specifies 256-bit AES
```

View information about the configuration by using the **show crypto isakmp policy** EXEC command.

crypto ipsec transform-set Command

Use the **crypto ipsec transform-set** command to define IPSec security protocols and algorithms.

```
crypto ipsec transform-set transform-set-name transform1 [transform2 transform3]
```

The accepted transform values are expanded. Under the category of Encapsulating Security Payload (ESP) Encryption Transform, one of the following can be chosen:

esp-aes ESP with the 128-bit AES encryption algorithm
esp-aes192 ESP with the 192-bit AES encryption algorithm
esp-aes256 ESP with the 256-bit AES encryption algorithm
esp-des ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
esp-3des ESP with the 168-bit 3DES encryption algorithm
esp-null null encryption algorithm

View information about the configuration by using the **show crypto ipsec transform-set** and **show crypto isakmp policy** EXEC commands.

Manual Certificate Enrollment

The TFTP and cut-and-paste (Manual Certificate Enrollment) generates a certificate request and accept certification authority (CA) certificates as well as the router certificates. These tasks are accomplished by using a TFTP server or manual cut-and-paste operations. Use TFTP or manual cut-and-paste enrollment in the following situations:

- The CA does not support Simple Certificate Enrollment Protocol (SCEP), the most commonly used method for sending and receiving requests and certificates.
- A network connection between the router and the CA is not possible.

Brief descriptions of some of the commands are provided in this section. A detailed explanation of the commands needed to configure Manual Certificate Enrollment can be found in the "Command Reference" section of Manual Certificate Enrollment (TFTP and Cut-and-Paste), and can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancrt.htm.

Manual Certificate Enrollment (TFTP and Cut-and-Paste) Prerequisites

TFTP and cut-and-paste enrollment has been added to the public key infrastructure (PKI) subsystem. The PKI subsystem requires the crypto subsystem.

Manual Certificate Enrollment (TFTP and Cut-and-Paste) Restrictions

You can switch between TFTP and cut-and-paste; for example, you can paste the CA certificate by using the **enrollment terminal** command, and then enter the **no enrollment terminal** and **enrollment url** *tftp://certserver/file_specification* commands to TFTP the requests and router certificates. However, Cisco does not recommend switching URLs if SCEP is used; that is, if the enrollment URL is "http://," *do not* change the enrollment URL between fetching the CA certificate and enrolling the certificate.

Manual Certificate Enrollment Concepts

This section describes the TFTP Certificate Enrollment and Cut-and-Paste Certificate Enrollment concepts.

TFTP Certificate Enrollment

A user might enable TFTP certificate enrollment if his or her CA does not support SCEP, which is the most commonly used method for sending and receiving requests and certificates. This feature takes the existing **enrollment ca-trustpoint** configuration subcommand and enhances the **url** *url* option to support TFTP certificate enrollment—**enrollment url** *tftp://certserver/file_specification*.

This subcommand specifies that TFTP should be used to send the enrollment requests and to retrieve the certificate of the CA and the certificate of the router. The *file_specification* is optional. However, if the *file_specification* is included in the URL, the router appends an extension to the file specification.

When the **crypto ca authenticate** command is entered, the router retrieves the certificate of the CA from the specified TFTP server. As appropriate, the router appends the extension ".ca" to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the router FQDN is used.) For example, if a user enters **enrollment url**

tftp://CA-server/TFTPfiles/router1, the TFTPfiles/router1.ca file is read from the TFTP server CA-server. If the router FQDN is router1.cisco.com, and you enter **enrollment url tftp://CA.cisco.com**, the router1.cisco.com.ca file is read from the TFTP server CA.cisco.com.

The file must contain the certificate of the CA in binary format or base 64 encoded.

When a user enrolls the router by using the **crypto ca enroll** command, he or she is prompted for information regarding the enrollment. The filename that is to be written is already determined at this point, and an extension of .req is appended to indicate that this is a certificate request.

For usage keys, two requests are generated and two certificates are expected to be granted. Thus, the extension for the certificate requests are -sign.req and -encr.req.

After the user enters the **crypto ca import** command, the router attempts to fetch the granted certificate by using TFTP and using the same filename that was used to send the request, except that .req extension is replaced by a .crt extension. (The certificates are expected to be base 64 encoded PCKS#10 format certificates.) The router parses the files it receives, verifies the certificates, and inserts the certificates into the internal certificate database.

Cut-and-Paste Certificate Enrollment

A user might want to manually cut-and-paste certificate enrollment requests and certificates when he or she does not have a network connection between the router and CA. Cut-and-paste enrollment introduces a new ca-trustpoint configuration subcommand—**enrollment**. This command should be used when configuring the trustpoint CA. After entering the **crypto ca enroll** command, you are asked the same questions about the IP address and serial number as a TFTP enrollment. The base 64 encoded certificate request is displayed on the terminal.

Similar to the TFTP process, the user enters the **crypto ca import** command to enter the granted certificate. With cut-and-paste, the base 64 encoded certificate is accepted from the console terminal. Certificate input ends after the user enters “quit” on a line by itself.

How to Configure Manual Certificate Enrollment

To enable manual certificate enrollment via TFTP or cut-and-paste, you must configure a trustpoint CA and the relevant enrollment tasks. This section contains the following procedures:

- Configuring Certificate Enrollment by Using TFTP
- Configuring Certificate Enrollment by Using Cut-and-Paste
- Verifying Manual Certificate Enrollment

Configuring Certificate Enrollment by Using TFTP

To declare the trustpoint CA that your router should use and to configure that trustpoint CA for manual enrollment by using TFTP, use the commands described in this section.

- You must know the correct URL to use if you are configuring certificate enrollment by using TFTP.
- The router must be able to write a file to the TFTP server for the **crypto ca enroll** command. Some TFTP servers require that the file exist on the server before it can be written. Most TFTP servers require that the file be writeable by the world. This requirement might pose a risk because any router or other device can write or overwrite the certificate request; in such a case, the router would not be able to use the certificate after it is granted by the CA because the request has been modified.

	Command or Action	Purpose
Step 1	**enable**	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**}	Enters global configuration mode.
Step 3	**crypto ca trustpoint** *name*	Declares the CA that your router should use and enters ca-trustpoint configuration mode.
Step 4	**enrollment** [**mode**] [**retry** *minutes*] [**retry** *number*] [**url** *url*]	Specifies the enrollment parameters of your CA. • **mode**—Specifies registration authority (RA) mode if your CA system provides a RA. • **retry** *minutes*—Specifies the wait period between certificate request retries. The default is 1 minute between retries. • **retry** *number*—Specifies the number of times that a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.) • **url** *url*—Specifies the URL of the CA to which your router should send certificate requests. If you are using SCEP for enrollment, *url* must be in the form http://CA_name, where CA_name is the CA's host Domain Name System (DNS) name or IP address. If you are using TFTP for enrollment, *url* must be in the form tftp://certserver/file_specification.
Step 5	**crypto ca authenticate** *name*	Takes the name of the CA as the argument.
Step 6	**exit**	Exits ca-trustpoint configuration mode and returns to global configuration.
Step 7	**crypto ca enroll** *name*	Obtains your router's certificate(s) from the CA.
Step 8	**crypto ca import** *name* **certificate**	Imports a certificate by using TFTP or manual cut-and-paste at the terminal.

Configuring Certificate Enrollment by Using Cut-and-Paste

To declare the trustpoint CA that your router should use and to configure that trustpoint CA for manual enrollment via cut-and-paste, use the commands described in this section.

	Command or Action	Purpose
Step 1	**enable**	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**}	Enters global configuration mode.
Step 3	**crypto ca trustpoint** *name*	Declares the CA that your router should use and enters ca-trustpoint configuration mode.
Step 4	**enrollment terminal**	Specifies manual cut-and-paste certificate enrollment.
Step 5	**crypto ca authenticate** *name*	Takes the name of the CA as the argument.

	Command or Action	Purpose
Step 6	**exit**	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	**crypto ca enroll** *name*	Obtains your router's certificate(s) from the CA.
Step 8	**crypto ca import** *name* **certificate**	Imports a certificate via TFTP or manually at the terminal. You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Certificate Enrollment Command Descriptions

crypto ca import Command

To import a certificate manually by using TFTP or cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode:

crypto ca import *name* **certificate**

where *name* **certificate** specifies the name of the CA. This name is the same name used when the certification authority (CA) was declared with the **crypto ca trustpoint** command (declares the CA that your router should use).

You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

enrollment terminal Command

To specify manual cut-and-paste certificate enrollment, use the enrollment terminal command in ca-trustpoint configuration mode.

enrollment terminal

To delete a current enrollment request, use the **no** form of this command.

enrollment Command

To specify the enrollment parameters of your certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode:

enrollment [mode] [retry minutes] [retry number] URL *url*

Where *url* specifies the URL of the CA where your router should send certificate requests. If you are using TFTP for enrollment, the URL must be in the form **tftp://***certserver/file_specification*. The *file_specification* is optional. If the *file_specification* is included in the URL, the router appends an extension to the file specification.

To remove any of the configured parameters, use the **no** form of this command.

Example of Manual Certificate Enrollment Configuration

The following example shows how to specify a manual cut-and-paste certificate enrollment by using the **enrollment terminal** subcommand of the **crypto ca trustpoint** command. In this example, the name of the trustpoint CA is "MS," and the **crypto ca import** command is entered twice because usage keys (signature and encryption keys) are used.

```
Router(config)# crypto ca trustpoint MS
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# crypto ca authenticate MS

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYS1yb290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0OFowOTELMAkG
A1UEBhMCVVMxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxEjAQBgNVBAMTCW1zY2Et
cm9vdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHpqxFuFhqyBnIC0OshIn9CtrdN3JvUNHr0NIKocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVR0PBAQDAgHGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FKIacsl6dKAfuNDVQymlSp7esf8jMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydEVucm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8v
XFxtc2NhLXJvb3RcQ2VydEVucm9sbFxtc2NhLXJvb3QuY3JsMBAGCSsGAQQBgjcV
AQQDAgEAMA0GCSqGSIb3DQEBBQUAA0EAeuZkZMX9qkoLHfETYTpVWjZPQbBmwNRA
oJDSdYdtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)#
Router(config)#crypto ca enroll MS
% Start certificate enrollment..

% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Display Certificate Request to terminal? [yes/no]:y
Signature key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdhXFDiWAn/hIZs9zfOtssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWyQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RxvONwx042pQchFnx9EkMuZC7evwRxJEqR
mBHXBZ8GmP3jYQsjS8MCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgeAMA0GCSqGSIb3DQEBBAUAA4GBAMT6WtyFw95POY7UtF+YIYHiVRUf4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCNid5Tov5jKogFHIki2EGGZxBosUw9lJlenQdNdDPbJc5LIWdfDvciA6jO
Nl8rOtKnt8Q+

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
```

```
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwG60QojpDbzbKnyj8FyTiOcv
THkDP7XD4vLT1XaJ409z0gSIoGnIcdFtXhVlBWtpq3/O9zYFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPqev7SPXpsAIsY8a6FMq7TiwLObqiQjLKL4cbuV0Frjl0Yuv5A/Z+
kqMOm7c+pWNWFdLe9lsCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgUgMA0GCSqGSIb3DQEBBAUAA4GBACF7feURj/fJMojPBlR6fa9BrlMJx+2F
H91YM/CIiz2n4mHTeWTWKhLoT8wUfa9NGOk7yi+nF/F7035twLfq6n2bSCTW4aem
8jLMMaeFxwkrV/ceQKrucmNC1uVx+fBy9rhnKx8j60XE25tnp1U08r6om/pBQABU
eNPFhozcaQ/2

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
n
Router(config)#crypto ca import MS certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0MloXDTAzMDYwODAxMjY0MlowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMXYVxQ4lgJ/4SGbPc3zrbLCgHWqFmLtJrPRXvz3sNNXYdeL13cYGnLL
TrNj6+cJOoyzj8ab8TiT1skDOoqS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdONqUHIRZ8fRJDLmQu3r8EcSRKkZgR1wWfBpj942ELI0vDAgMBAAGjggHM
MIIByDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFL8Quz8dyz4EGIeKx9A8UMNHLE4s
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTQX2EDoJpR/A2UHXxRYqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3WOjz9wZo=

% Router Certificate successfully imported

Router(config)#
Router(config)#crypto ca import MS certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0NVoXDTAzMDYwODAxMjY0NVowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMButEKI6Q282yp8o/Bck4jnL0x5Az+1w+Ly09V2ieNPc9IEiKBpyHHR
bV4VZQVraat/zvc2BV69bR/gTAkUIty7bNCKcWGtw/YhT6nr+0j16bACLGPGuhTK
u04sCzm6okIyyi+HG7ldBa45dGLr+QP2fpKjDpu3PqVjVhXS3vZbAgMBAAGjggHM
MIIByDALBgNVHQ8EBAMCBSAwHQYDVR0OBBYEFPDO29oRdlEUSgBMg6jZR+YFRWlj
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
```

```
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAHaU
hyCwLirUghNxCmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdMNPPyApuh8SoT2zBP
ZKjZU2WjcZG/nZF4W5k=

% Router Certificate successfully imported
```

Verifying Manual Certificate Enrollment

To verify that the Manual Certificate Enrollment feature is working, perform the following optional steps:

	Command or Action	Purpose
Step 1	**enable**	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show crypto ca certificates**	(Optional) Verifies information about your certificate, the certificate of the CA, and RA certificates.
Step 3	**show crypto ca trustpoints**	(Optional) Displays the trustpoints that are configured in the router.

The following sample output is displayed after manual certificate enrollment has been successfully configured by using the **enrollment terminal** command (cut-and-paste):

```
Router# show crypto ca certificates

Certificate
  Status:Available
  Certificate Serial Number:14DECE05000000000C48
  Certificate Usage:Encryption
  Issuer:
    CN = msca-root
     O = Cisco Systems
     C = US
  Subject:
    Name:Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root/CertEnroll/msca-root.crl
  Validity Date:
    start date:18:16:45 PDT Jun 7 2002
    end   date:18:26:45 PDT Jun 7 2003
    renew date:16:00:00 PST Dec 31 1969
  Associated Trustpoints:MS

Certificate
  Status:Available
  Certificate Serial Number:14DEC2E9000000000C47
  Certificate Usage:Signature
  Issuer:
    CN = msca-root
     O = Cisco Systems
     C = US
  Subject:
    Name:Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root/CertEnroll/msca-root.crl
```

```
  Validity Date:
    start date:18:16:42 PDT Jun 7 2002
    end   date:18:26:42 PDT Jun 7 2003
    renew date:16:00:00 PST Dec 31 1969
  Associated Trustpoints:MS

CA Certificate
  Status:Available
  Certificate Serial Number:3AC0A65E9547C2874AAF2468A942D5EE
  Certificate Usage:Signature
  Issuer:
    CN = msca-root
     O = Cisco Systems
     C = US
  Subject:
    CN = msca-root
     O = Cisco Systems
     C = US
  CRL Distribution Point:
    http://msca-root/CertEnroll/msca-root.crl
  Validity Date:
    start date:16:46:01 PST Feb 13 2002
    end   date:16:54:48 PST Feb 13 2007
  Associated Trustpoints:MS
```

Related Documents

Table 9-1 shows documents that contain additional information on Mobile IP Security.

Table 9-1 Documents Related to Mobile IP Security

Related Topic	Document Title
CA configuration tasks	The chapter "Configuring Certification Authority Interoperability" in the *Cisco IOS Security Configuration Guide*, Release 12.2
Additional certificate and CA commands	The chapter "Certification Authority Interoperability Commands" in the *Cisco IOS Security Command Reference*, Release 12.2
Additional ca-trustpoint configuration commands	*Trustpoint CLI*, Cisco IOS Release 12.2(8)T feature module

CHAPTER 10

Zeroization

Zeroization erases all potentially sensitive information in the router memory. This includes the erasure of the main memory, cache memories, and other memories containing packet data, NVRAM, and Flash. Zeroization is launched by taking an action. Typically, there is a button on the faceplate that invokes zeroization. The result of that action is determined by the configuration of the router. The parameters for zeroization can be configured, but zeroization cannot be invoked through the command–line interface (CLI).

Caution Zeroization is disabled by default. When zeroization is enabled, the AUX port should not be used for any function other than an actuator, such as a push button. There is no way to reliably ascertain whether a device connected to the AUX port might trigger zeroization. We recommend that if zeroization is enabled, no devices, with the exception of the zeroization actuator, be attached to the AUX port. There are some AUX port configuration restrictions when zeroization is enabled.

Zeroization can only be invoked and executed locally. It cannot be invoked and executed remotely through a Telnet session. The time needed for zeroizing is about 5 minutes.

Some items cannot be completely scrubbed because the devices provide a *reset* or *invalidate* of the memory, rather than providing a full data path through which the scrubbing patterns can be written.

These items are scrubbed:

- Dual–port RAM in the CPM
- Main memory

All the main memory is scrubbed except the memory area containing a small program loop that does the actual scrubbing. Scrubbing is defined as performing several passes through the memory areas, overwriting the memory using a separate data pattern for each pass.

These items cannot be scrubbed:

- Console and AUX port UART FIFOs. A series of characters is forced through the FIFOs to ensure that all sensitive information in the FIFOs is flushed.
- NVRAM, which is erased entirely.
- Flash file system, which is erased entirely.
- Caches, that are flushed and invalidated, eliminating all of the information. The process of scrubbing the main memory causes all cache lines to receive the scrubbing data patterns.

The data patterns used for scrubbing consist of separate passes; each pass fills the memory with the following data patterns:

- All ones (e.g. 0xffff ffff)
- Alternating ones and zeroes (e.g. 0xa5a5 a5a5)
- Alternating zeroes and ones (e.g. 0x5a5a 5a5a)
- All zeroes (e.g. 0x0000 0000)

The data patterns ensure that

- Each bit in the memory is cleared to zero and set to one at least once.
- The final state of the memory is such that all prior information is erased.

Some items cannot be completely scrubbed. For example, some devices provide a *reset* or *invalidate* of their memory, rather than providing a full data path through which the scrubbing patterns can be written.

In addition, zeroization shuts down all network interfaces, and causes zeroization of the Cisco IOS configuration and object code files, including all IP addresses on the router that are contained in volatile memory.

Note The procedures for enabling Zeroization have been left out of this document intentionally for legal reasons. Please contact your system integrator for more information.

End User Interface

The user interface consists of configuration and show commands.

service declassify command

Enter the **service declassify** command to enable the declassification function and monitor the AUX port CTS pin. Entering the **no** form of this command disables the declassification function and AUX port monitoring. If a parameter is not specified, neither the Flash file system nor the NVRAM is declassified (erased).

Syntax Description **[no] service declassify {erase-flash | erase-nvram | erase-all}**

erase-flash	(Optional) Erases all files in the Flash file system when declassification is invoked.
erase-nvram	(Optional) Erases all files in the NVRAM file system when declassification is invoked.
erase-all	(Optional) Scrubs and erases all files on the router when declassification is invoked

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
12.3(8)TD	This command was introduced.

Usage Guidelines The network interfaces are shut down when declassification is invoked.

No CLI command invokes the declassification process. Declassification is invoked by using an external signal that appears on the AUX port of the router. When declassification is complete, the ROMMON prompt appears on the console.

The output that appears on the console when declassification is initiated depends on what options have been configured. It is not possible to document exactly what appears on the screen, because of the complex interactions between the declassification process and the logging process during declassification.

Examples The following examples show the console output when declassification is invoked.

erase-all

The output on the console when the **erase-all** parameter is set resembles the following:

```
Router#service declassify erase-all

*Mar  5 17:44:28.347:
Declassification initiated...
*Mar  5 17:44:30.647: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  5 17:44:31.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to downÿ
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note If the **service declassify erase-all** is configured and the Flash file system is erased, error recovery actions must be initiated to load a bootable image on the router. The startup configuration file is also erased; the router boots from the factory default configuration the next time it is booted.

erase-flash

The output on the console when the **erase-flash** parameter is set resembles the following:

```
Router#service declassify erase-flash

*Mar  1 00:01:30.091:
Declassification initiated...
*Mar  1 00:01:34.347: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  1 00:01:35.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
```

```
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note The flash file system is erased and there will not be a bootable image for the router in the Flash file system if the **service declassify erase-flash** is configured. Error recovery actions must be initiated to load a bootable image.

The startup configuration file is not erased if the **service declassify erase-flash** is configured. When the router is booted, it is configured using its startup configuration file in NVRAM.

erase-nvram

The output on the console when the **erase-nvram** parameter is set resembles the following:

```
Router#service declassify erase-nvram
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory

rommon 1 >
```

Note If the **service declassify erase-nvram** is configured, the flash file system is not erased. The bootable image in the Flash file system remains and the router can be booted. The startup configuration file is erased; because the router has no configuration file, it boots from the default configuration.

Related Commands

Command	Description
show declassify	Displays the state of the **service declassify** command.

show declassify

Enter the **show declassify** command to display the state of the declassify function (enabled, in-progress, and so forth), and the sequence of declassification steps that will be performed.

show declassify

Command Modes Global configuration

Command History

Release	Modification
12.3(8)TD	This command was introduced.

Examples

The following is sample output for the **show declassify** command:

```
router#show declassify
Router#show declassify
    Declassify facility: Enabled=Yes  In Progress=No
    Erase flash=Yes  Erase nvram=Yes
    Obtain memory size
    Shutdown Interfaces
    Declassify Console and Aux Ports
    Erase flash
    Declassify NVRAM
    Declassify Communications Processor Module
    Declassify RAM, D-Cache, and I-Cache
```

Related Commands

Command	Description
service declassify	Invokes declassification.

Redundancy in a Mobile Environment

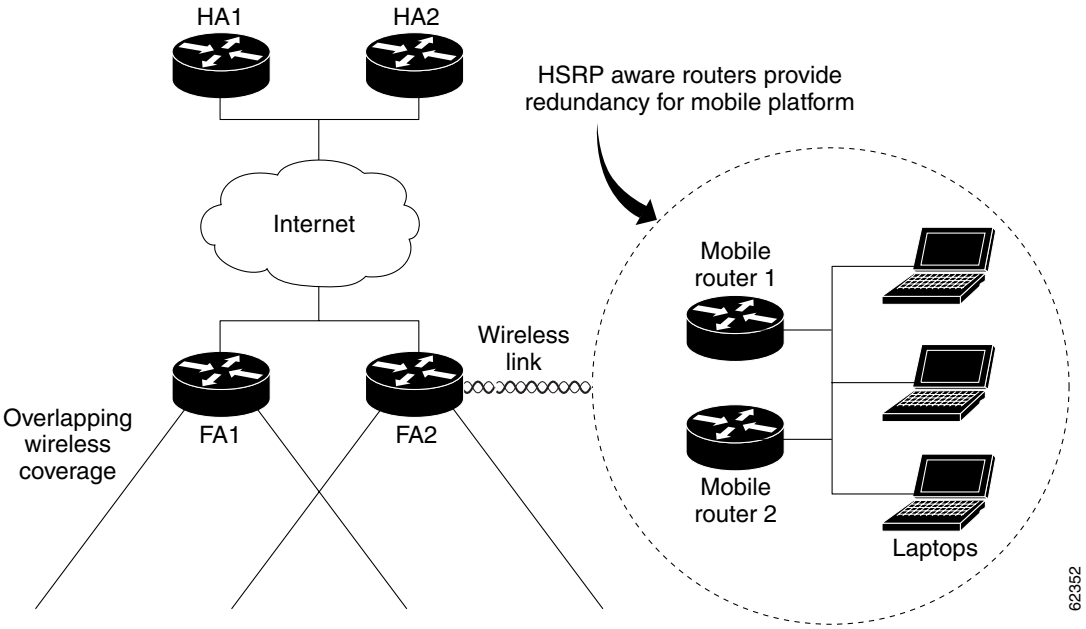
There can be three levels of redundancy for the Cisco Mobile Network: mobile access router (MR) redundancy, home agent (HA) redundancy, and foreign agent (FA) redundancy. Hot Standby Router Protocol (HSRP) need not be configured on the Foreign Agent. Foreign Agent redundancy is achieved by overlapping wireless coverage.

This chapter describes advanced mobile access router redundancy configurations.

Mobile Access Router Redundancy

Mobile access router redundancy provides backup for Mobile Networks if the mobile access router goes down. A passive mobile access router detects if an active mobile access router goes down, by using interface tracking and HSRP. Once a passive mobile access router detects that an active mobile access router is down, it sends a registration request to create a new binding and take over as the active mobile access router. The passive mobile access router is in an isolated state until it becomes active.

Figure 11-1 Mobile Access Router Redundancy



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

	Command	Purpose
Step 1	`Router(config-if)# standby [group-number] ip [ip-address [secondary]]`	Enables the HSRP.
Step 2	`Router(config-if)# standby priority priority`	Sets the Hot Standby priority used in choosing the active router.
Step 3	`Router(config-if)# standby preempt`	Configures the router to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router.
Step 4	`Router(config-if)# standby name group-name`	Configures the name of the standby group.
Step 5	`Router(config-if)# standby [group-number] track interface-type interface-number [interface-priority]`	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces. The *interface-priority* argument specifies the amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.
Step 6	`Router(config-if)# exit`	Exits interface configuration mode.
Step 7	`Router(config)# ip mobile router`	Enables the mobile access router.
Step 8	`Router(mobile-router)# redundancy group name`	Configures fault tolerance for the mobile access router. The *name* argument must match the name specified in the **standby name** *group-name* command.

You do not need to configure HSRP on both the mobile access router roaming interface and the interface attached to the physical mobile networks. If one of the interfaces is configured with HSRP, and the **standby track** command is configured on the other interface, the redundancy mechanism will work.

Mobile Access Router Redundancy Example

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

Mobile Router 1

```
interface loopback0
 ip address 10.1.0.1 255.255.255.255
router mobile
ip mobile router
 address 10.1.0.1 255.255.0.0
 home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 101 key hex 12345678123456781234567812345678
!
interface serial 0
!Roaming interface and periodic solicitation
 ip mobile router-service roam
 ip mobile router-service solicit
interface ethernet 0
 ip mobile router-service roam
```

```
interface ethernet 1
 ip address 10.1.1.1 255.255.255.0
interface ethernet 2
 ip address 10.1.2.1 255.255.255.0
```

Mobile Router 2

```
interface loopback0
 ip address 10.2.0.1 255.255.255.255
router mobile
ip mobile router
 address 10.2.0.1 255.255.0.0
 home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781
!
interface serial 0
!Roaming interface and periodic solicitation
 ip mobile router-service roam
 ip mobile router-service solicit
interface ethernet 0
 ip mobile router-service roam
interface ethernet 1
ip address 10.2.1.1 255.255.255.0
interface ethernet 2
 ip address 10.2.2.1 255.255.255.0
```

Home Agent Redundancy

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

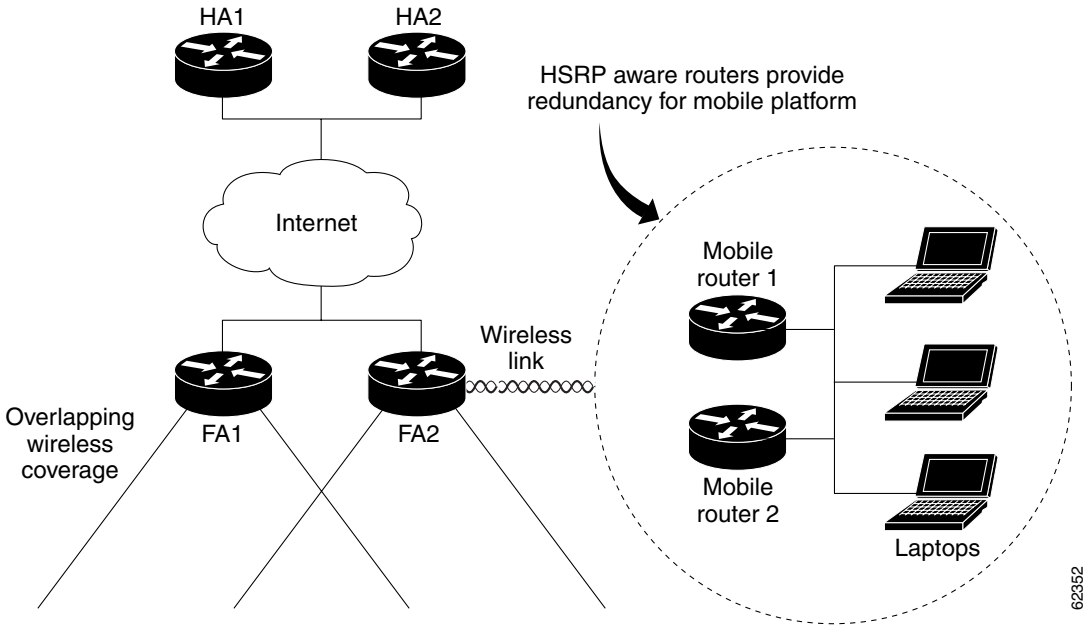
The mobile networks also are defined on the home agent so that the home agent knows to inject these networks into the routing table when the mobile access router is registered.

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

The mobile access routers use HSRP to provide redundancy, and their group name is associated to the HSRP group name. The mobile access routers are aware of the HSRP states. When HSRP is in the active state, the mobile access router is active. If HSRP is in the nonactive state, the mobile access router is passive.

See Figure 11-2 for an example topology of a redundant network.

Figure 11-2 Topology Showing Cisco Mobile Network Redundancy



HA1

```
interface Ethernet0/0
 ip address 100.100.100.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 100.100.100.100
 standby priority 100
 standby preempt delay sync 5
!HSRP group name
 standby name HA_HSRP2
!
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent address 100.100.100.100
!Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
```

```
ip mobile mobile-networks 70.70.70.70
 description san jose jet
!Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.2 spi 300 key ascii hi
```

HA2

```
interface Ethernet1/1
 ip address 100.100.100.2 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 standby ip 100.100.100.100
 standby priority 99
 standby preempt delay sync 5
!HSRP group name
 standby name HA_HSRP2
!
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent address 100.100.100.100
!Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
ip mobile mobile-networks 70.70.70.70
 description san jose jet
!Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.1 spi 300 key ascii hi
```

Home Agent Redundancy Configuration

The home agent creates a mobility binding table that tracks the association of a home address with the current care-of address of the mobile node. However, if the home agent fails, the mobility binding table will be lost and all mobile nodes registered with the home agent lose connectivity unless a redundancy mechanism is employed.

The Mobile IP home agent Redundancy feature runs on top of the HSRP and designates one active home agent and a standby home agent. HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic will immediately and transparently recover from first hop failures in network edge devices.

By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router or default gateway to the hosts on a LAN. The members of the router group continually exchange status messages by detecting when a router goes down. This router group is referred to as the HSRP group.

The Mobile IP home agent redundancy functionality allows standby home agents and active home agents to exchange mobility binding updates. Also, when a router first becomes the standby home agent, the active home agent downloads the entire mobility binding table to the standby home agent.

The following sections give an overview of how redundancy is implemented when a mobile node travels to a foreign network.

Registration and Mobility Binding Tables

Without home agent redundancy, the mobility binding table entries are not communicated to the standby home agent. If the active home agent fails, the mobility binding table is lost and all mobile nodes registered to the home agent lose connectivity.

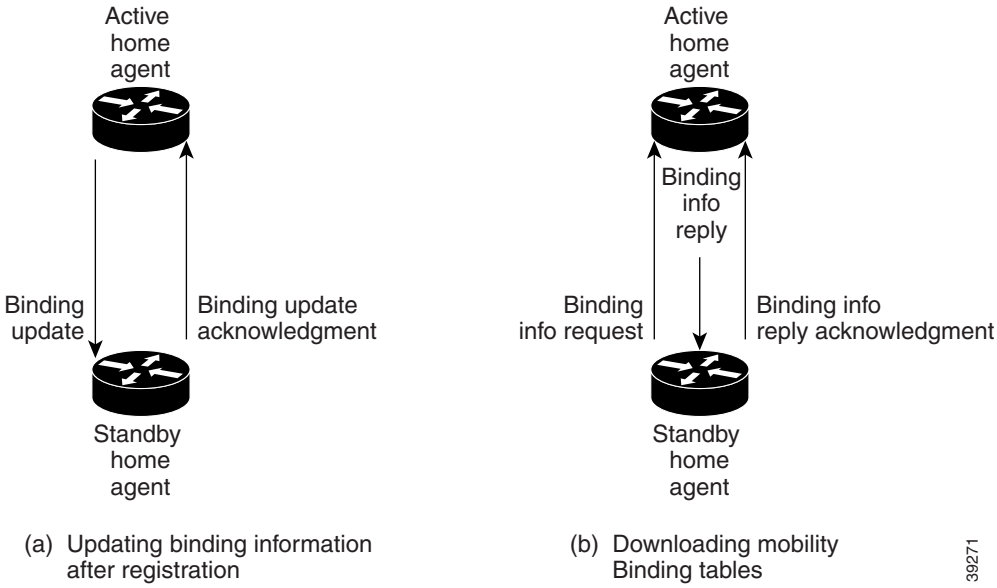
Home agent functionality is a service provided by the router and is not interface specific. The main concern is on which interface of the home agent should a mobile node use to send its registration requests, or alternatively, on which interface of the home agent should the home agent receive registration requests. There are two scenarios to consider: (1) a mobile node that has an home agent interface (home agent IP address) that is not on the same subnet as the mobile node, and (2) a mobile node that requires the home agent interface to be on the same subnet as the mobile node, that is, the home agent and mobile node must be on the same home network. Note that the choice of which home agent IP address to use is an agreement between the home agent and mobile node.

For mobile nodes on physical networks, an active home agent accepts registration requests from the mobile node and sends the binding updates to the standby home agent. This process keeps the mobility binding table synchronized between the standby home agent and active home agent. See Figure 11-3(a) for an example of this process.

Virtual networks are logical circuits that are programmed and share a common physical infrastructure. For this type of network, the active and standby home agents are peers—either can handle registration requests and update the peer home agent.

When a standby home agent comes up, it must request all mobility binding information from the active home agent. The active home agent responds by downloading the mobility binding table to the standby home agent. The standby home agent acknowledges that it has received the requested binding information. See Figure 11-3(b) for an example of an active home agent downloading the mobility bindings to a standby home agent. A main concern in this scenario is which home agent IP address should the standby home agent use to retrieve the appropriate mobility binding table and on which interface of the standby home agent should the binding request be sent.

Figure 11-3 Mobility Binding Process



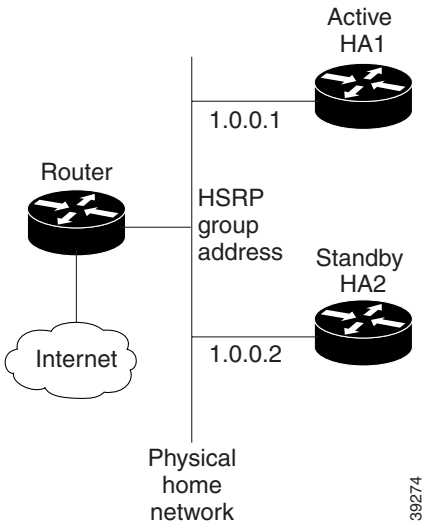
Home Agent Redundancy on a Physical Network

To enable home agent redundancy for a physical network, complete the following procedure:

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

Figure 11-4 shows an example network topology for physical networks. The configuration example supports home agents that are on the same or a different physical network as the mobile node.

Figure 11-4 Topology Showing Home Agent Redundancy on a Physical Network



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

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

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

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

Active HA1:

```
int Ethernet0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110

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

Standby HA2:

```
int Ethernet0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

 ip mobile home-agent standby SanJoseHA
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Home Agent Redundancy on a Virtual Network Using One Physical Network

To enable home agent redundancy for a virtual network using one physical network, complete the following procedure:

	Command	Purpose
Step 1	`Router (config)# standby [hsrp-group-number] ip hsrp-group-addr`	Enable the HSRP.
Step 2	`Router(config)# standby name hsrp-group-name`	Configure the name of the standby group.
Step 3a	`Router(config)# ip mobile home-agent address hsrp-group-addr`	Define a global home agent address. Execute Step 3a when the the mobile node and home agent are on different subnets.
Step 3b	`Router(config)# ip mobile home-agent`	Enable and control home agent services to the router. Execute Step 3b when the mobile node and home agent are on the same subnet.
Step 4	`Router(config)# ip mobile virtual-network net mask [address addr]`	Define the virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *addr*] option.
Step 5	`Router(config)# ip mobile home-agent standby hsrp-group-name [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group to support virtual networks.
Step 6	`Router(config)# ip mobile secure home-agent addr spi spi key hex string`	Configure the home agent security association between peer routers. If configured on the active home agent, the IP address *addr* is that of the standby home agent. If configured on the standby home agent, the IP address *addr* is that of the active router. Note that a security association must be set up between all home agents in the standby group.

Example of a Virtual Network Using One Physical Network

This section presents two configuration examples: the mobile node and home agent are on different subnets, and the mobile node and home agent are on the same subnet.

Note A maximum of one FESMIC is supported per router.

Different Subnets

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

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

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

Active HA1:

```
int fe0/0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

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

Standby HA2:

```
int e0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

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

Same Subnet

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

Active HA1:

```
int fe0/0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

! loopback to receive registration from MN on virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255

ip mobile home-agent
! address used by Standby home agent for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 hex 00112233445566778899001122334455
```

Standby HA2:

```
int e0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

! loopback to receive registration from MN on virtual-network
 int lo0
 ip addr 20.0.0.1 255.255.255.255

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

Home Agent Redundancy on a Virtual Network Using Multiple Physical Networks

To enable home agent redundancy for a virtual network using multiple physical network, complete the following procedure:

	Command	Purpose
Step 1	`Router (config-if)# standby [hsrp-group-number] ip hsrp-group-addr`	Enable the HSRP.
Step 2	`Router(config-if)# standby [standby-group-number] name hsrp-group-name1`	Configure the name of the standby HSRP group1.
Step 3	`Router(config-if)# standby [standby-group-number] name hsrp-group-name2`	Configure the name of the standby HSRP group2.
Step 4	`Router(config-if)# standby [group-number] priority priority1`	Configure the name of the priority HSRP group1, that prioritizes a potential hot standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.
Step 5	`Router(config-if)# standby [group-number] priority priority2`	Configure the name of the priority HSRP group2.

	Command	Purpose
Step 6a	`Router(config)# ip mobile home-agent address loopback-interface-addr`	Define the global home agent address for virtual networks. In this configuration, the address is the loopback interface address. Execute Step 6a if the mobile node and home agent are on different subnets.
Step 4b	`Router(config)# ip mobile home-agent`	Enable and control home agent services. Execute Step 4b if the mobile node and home agent are on the same subnet.
Step 5	`Router(config)# ip mobile virtual-network net mask [address addr]`	Define the virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *addr*] option.
Step 6	`Router(config)# ip mobile home-agent standby hsrp-group-name1 [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group1 to support virtual networks.
Step 7	`Router(config)# ip mobile home-agent standby hsrp-group-name2 [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group2 to support virtual networks.
Step 8	`Router(config)# ip mobile secure home-agent addr spi spi key hex string`	Configure the home agent security association between peer routers. If configured on the active home agent, the IP address *addr* is that of the standby home agent. If configured on the standby home agent, the IP address *addr* is that of the active router. Note that a security association must be set up between all home agents in the standby group.

Example of HA Redundancy for a Virtual Network Using Multiple Physical Networks

This section presents two configuration examples: the mobile node and home agent are on different subnets, and the mobile node and home agent are on the same subnet.

Different Subnets

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

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

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

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

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

Active HA1:

```
int e0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int e1
 ip addr 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

int lo0
 ip addr 10.0.0.10 255.255.255.255

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

Standby HA2:

```
int e0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int e1
 ip addr 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

int lo0
 ip addr 10.0.0.10 255.255.255.255

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

Same Subnet

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

Active HA1

```
int e0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int e1
 ip addr 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

! loopback to receive registration from MN on virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255

 ip mobile home-agent
! address used by Standby home agent for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

Active HA2

```
int e0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

int e1
 ip addr 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

! loopback to receive registration from MN on virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255

 ip mobile home-agent
! address used by Standby home agent for redundancy (update and download)
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Home Agent Redundancy on Multiple Virtual Networks Using One Physical Network

To enable home agent redundancy for multiple virtual networks using one physical network, complete the following procedure:

	Command	Purpose
Step 1	`Router(config-if)# standby [hsrp-group-number] ip hsrp-group-addr`	Enable the HSRP.
Step 2	`Router(config-if)# standby name hsrp-group-name`	Configure the name of the standby group.

	Command	Purpose
Step 3a	`Router(config)# ip mobile home-agent address hsrp-group-addr`	Define a global home agent address. Execute Step 3a when the the mobile node and home agent are on different subnets.
Step 3b	`Router(config)# ip mobile home-agent`	Enable and control home agent services to the router. Execute Step 3b when the mobile node and home agent are on the same subnet.
Step 4	`Router(config)# ip mobile virtual-network net mask [address addr]`	Define the virtual networks. Repeat this step for each virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *addr*] option.
Step 5	`Router(config)# ip mobile home-agent standby hsrp-group-name [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group to support virtual networks.
Step 6	`Router(config)# ip mobile secure home-agent addr spi spi key hex string`	Set up the home agent security association between peer routers. If configured on the active home agent, the IP address *addr* is that of the standby home agent. If configured on the standby home agent, the IP address *addr* is that of the active router. Note that a security association must be set up between all home agents in the standby group.

Example of Multiple Virtual Networks Using One Physical Network

This section presents two configuration examples: the mobile node and home agent are on different subnets, and the mobile node and home agent are on the same subnet. Figure 11-5 shows an example network topology for example. Figure 11-6 shows an example network topology for example.

Figure 11-5 Topology Showing Home Agent Redundancy on Multiple Virtual Networks Using One Physical Network (Different Subnets)

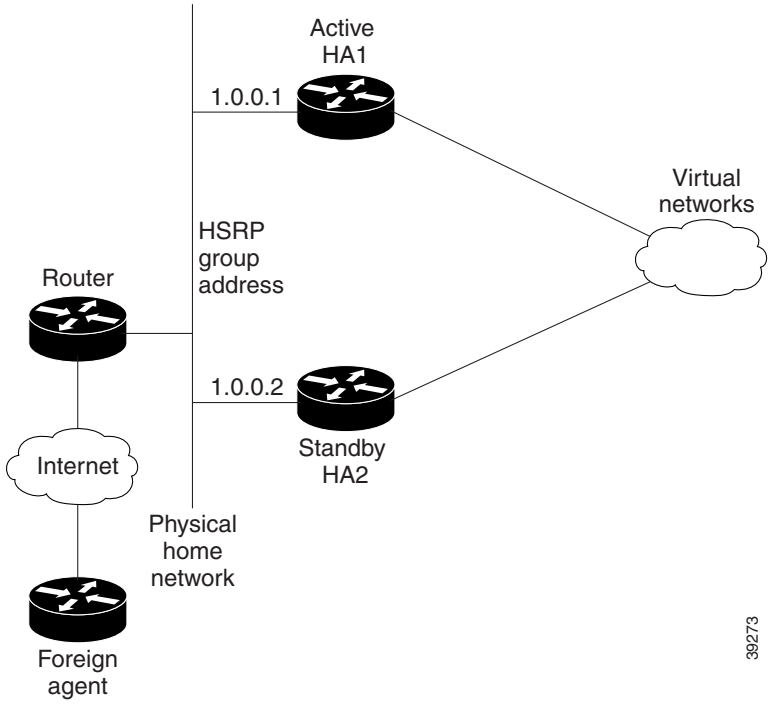
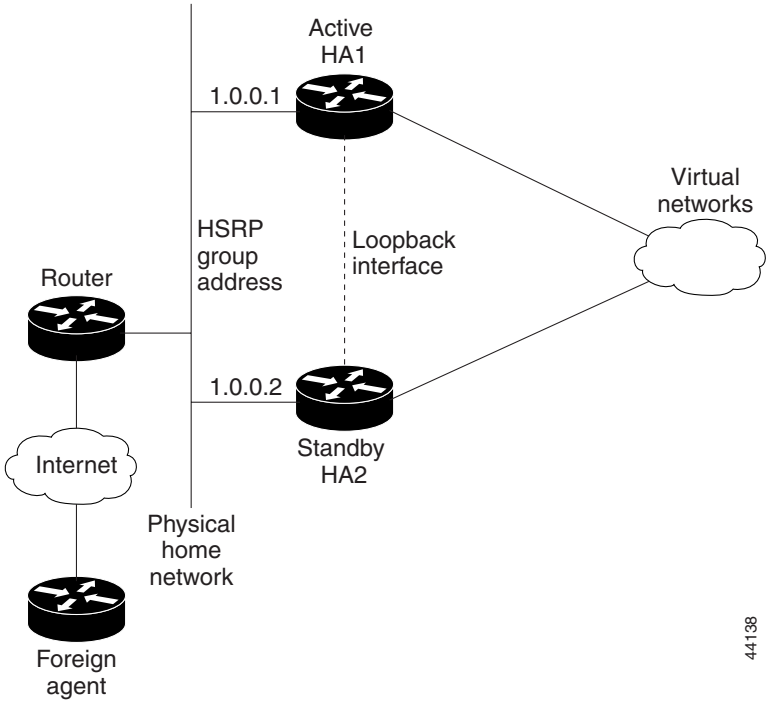


Figure 11-6 Topology Showing Home Agent Redundancy on Multiple Virtual Networks Using One Physical Network (Same Subnet)



Different Subnets

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

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

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

Active HA1:

```
int e0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

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

Standby HA2:

```
int e0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

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

Same Subnet

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

Active HA1

```
int Ethernet0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

! loopback to receive registration from MN on each virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255
 ip addr 30.0.0.1 255.255.255.255 secondary

 ip mobile home-agent
! address used by Standby home agent for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

Standby HA2

```
int Ethernet0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

! loopback to receive registration from MN on each virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255
 ip addr 30.0.0.1 255.255.255.255 secondary
```

```
ip mobile home-agent
! address used by Standby home agent for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
! used to map to the HSRP group SanJoseHA
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Home Agent Redundancy on Multiple Virtual Networks Using Multiple Physical Networks

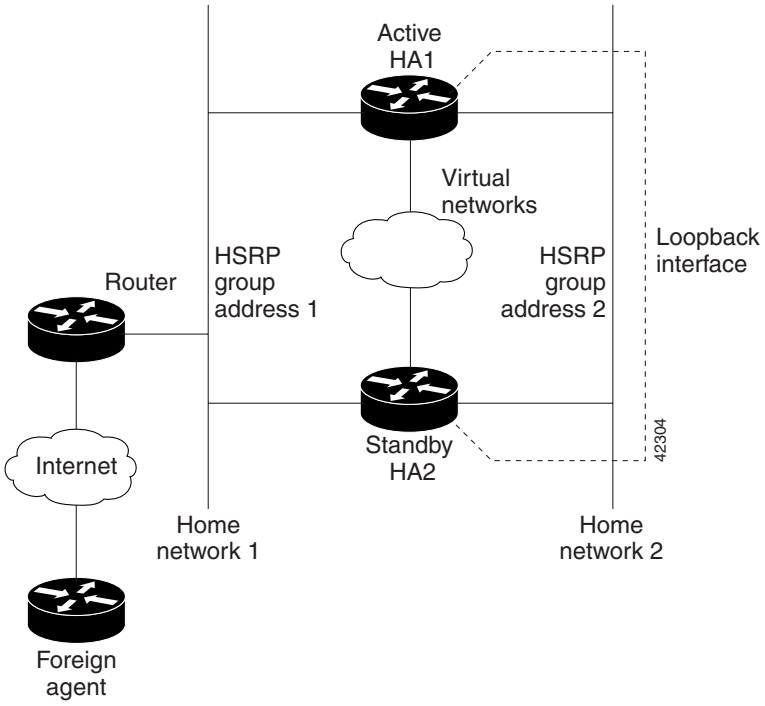
To enable home agent redundancy for multiple virtual network using multiple physical networks, complete the following procedure:

	Command	Purpose
Step 1	`Router (config-if)# standby [hsrp-group-number] ip hsrp-group-addr`	Enable the HSRP.
Step 2	`Router(config-if)# standby name hsrp-group-name1`	Configure the name of the standby HSRP group1.
Step 3	`Router(config-if)# standby name hsrp-group-name2`	Configure the name of the standby HSRP group2.
Step 4a	`Router(config)# ip mobile home-agent address loopback-interface-addr`	Execute Step 4a if the mobile node and home agent are on different subnets. Define the global home agent address for virtual networks. In this configuration, the address is the loopback interface address.
Step 4b	`Router(config)# ip mobile home-agent`	Execute Step 4b if the mobile node and home agent are on the same subnet. Enable and control home agent services.
Step 5	`Router(config)# ip mobile virtual-network net mask [address addr]`	Define the virtual networks. Repeat this step for each virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *addr*] option.
Step 6	`Router(config)# ip mobile home-agent standby hsrp-group-name1 [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group1 to support virtual networks.
Step 7	`Router(config)# ip mobile home-agent standby hsrp-group-name2 [[virtual-network] address addr]`	Configure the home agent for redundancy using the HSRP group2 to support virtual networks.
Step 8	`Router(config)# ip mobile secure home-agent addr spi spi key hex string`	Set up the home agent security association between peer routers. If configured on the active home agent, the IP address *addr* is that of the standby home agent. If configured on the standby home agent, the IP address *addr* is that of the active router. Note that a security association must be set up between all home agents in the standby group.

Example of Multiple Virtual Networks Using Multiple Physical Networks

Figure 11-7 shows an example network topology for this configuration type. This section presents two configuration examples: (1) the mobile node and home agent are on different subnets, and (2) the mobile node and home agent are on the same subnet.

Figure 11-7 Topology Showing Home Agent Redundancy on Virtual Networks Using Multiple Physical Networks



Different Subnets

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

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

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

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

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

Active HA1:

```
int Ethernet0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int Ethernet0
 ip addr 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

int lo0
 ip addr 10.0.0.10 255.255.255.255

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

Standby HA2:

```
int Ethernet0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int Ethernet1
 ip addr 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

int lo0
 ip addr 10.0.0.10 255.255.255.255

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

Same Subnet

For each virtual network, a loopback address is configured on the home agent to be on the same subnet as the virtual network. It is only necessary to configure one loopback interface, and assign different IP addresses to the loopback interface for each virtual network, that is, using the **ip address** *ip-address mask* [**secondary**] command.

A mobile node on a particular virtual network will use home agent IP address =loopback address configured for that virtual network. When a standby home agent comes up, it will also use this home agent IP address to retrieve mobility bindings for mobile nodes on a particular virtual network.

Active HA1

```
int Ethernet0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHANet1

int Ethernet1
 ip addr 2.0.0.1 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

! loopback to receive registration from MN on each virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255
 ip addr 30.0.0.1 255.255.255.255 secondary
 ip addr 40.0.0.1 255.255.255.255 secondary

ip mobile home-agent
! address used by Standby home agent for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
 ip mobile virtual-network 40.0.0.0 255.0.0.0 address 40.0.0.1
! used to map to the HSRP groups SanJoseHANet1 and SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.2 spi 100 key hex 00112233445566778899001122334455
```

Standby HA2

```
int Ethernet0
 ip addr 1.0.0.2 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

int Ethernet1
 ip addr 2.0.0.2 255.0.0.0
 standby ip 2.0.0.10
 standby name SanJoseHANet2

! loopback to receive registration from MN on each virtual-network
int lo0
 ip addr 20.0.0.1 255.255.255.255
 ip addr 30.0.0.1 255.255.255.255 secondary
 ip addr 40.0.0.1 255.255.255.255 secondary
```

```
ip mobile home-agent
! address used by Standby home agent for redundancy (update and download) for
! each virtual-network
 ip mobile virtual-network 20.0.0.0 255.0.0.0 address 20.0.0.1
 ip mobile virtual-network 30.0.0.0 255.0.0.0 address 30.0.0.1
 ip mobile virtual-network 40.0.0.0 255.0.0.0 address 40.0.0.1
! used to map to the HSRP groups SanJoseHANet1 and SanJoseHANet2
 ip mobile home-agent standby SanJoseHANet1 virtual-network
 ip mobile home-agent standby SanJoseHANet2 virtual-network
 ip mobile secure home-agent 1.0.0.1 spi 100 key hex 00112233445566778899001122334455
 ip mobile secure home-agent 2.0.0.1 spi 100 key hex 00112233445566778899001122334455
```

Redundancy Verification

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

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

Quality of Service for Cisco 3200 Routers

QOS can be used to manage the output interface to increase efficiency by prioritizing the traffic. When the output interface is fast (for example, a Fast Ethernet connecting a single client), the probability of the packets being dropped or delayed is very low. When the output interface is slow, heavy traffic on the output interface causes congestion, resulting in dropped and delayed packets. An interface connected to an intermediate device, such as a WMIC, that forwards traffic to a slow uplink interface should have QOS configured.

QoS is a measure of performance that reflects router transmission quality and service availability. The mobile access router supports the following QoS features:

QoS Features Supported

Table 12-1 shows the QoS features supported by the Cisco 3200 Series router.

Table 12-1 Supported QoS Features

Feature	Serial	FastEthernet 0/0	SVI-VLAN Interface
Class-based Weighted Fair Queueing (CBWFQ)	Yes	Yes	Yes[1]
Network Based Application Recognition (NBAR)	Yes	Yes	Yes
Class Based Packet Marking—Setting IP Precedence bits	Yes	Yes	Yes
Class Based Packet Marking—QoS Group Value	Yes	Yes	Yes
Class Based Packet Marking—Differentiated Services Code Point (DSCP)	Yes	Yes	Yes
Class Based Policer for the DSCP	Yes	Yes	Yes
Class Based Ethernet Class of Service (CoS) Matching and Marking (802.1p COS)	Yes	Yes	No
Priority Queueing	Yes	Yes	No[1]
Traffic Policing	Yes	Yes	Yes
Class Based Policer for the DiffServ Assured Forwarding (AF) Per Hop Behavior	Yes	Yes	Yes
Link Fragmentation and Interleaving (LFI)	Yes	N/A	N/A
Weighted Random Early Detection (WRED)	Yes	Yes	Yes[1]

Table 12-1 Supported QoS Features (continued)

Feature	Serial	FastEthernet 0/0	SVI-VLAN Interface
DiffServ Compliant WRED	Yes	Yes	Yes[1]
Flow Based WRED	Yes	Yes	Yes[1]
Random Early Detection (RED)	Yes	Yes	Yes[1]
Low Latency Queueing (LLQ)	Yes	Yes	Yes[1]
LLQ for Frame Relay	Yes	N/A	N/A
Custom Queueing	Yes	Yes	No[1]
Weighted Fair Queueing (WFQ)	Yes	Yes	Yes[1]
Committed Access Rate (CAR)	Yes	Yes	Yes
Generic Traffic Shaping (GTS)	Yes	Yes	Yes

1. See the "QoS Restrictions" section in this chapter.

QoS Restrictions

When configuring the Switch Virtual Interface (SVI) on the FESMIC, the interface is not required to provide a mechanism for notifying the router that it has become congested for the QoS features shown in Table 12-2 to work properly. To work around this restriction, a Class Based Traffic Shaping with a Hierarchical (Nested) Policy Map must be configured on the SVI. Configuring Class Based Traffic Shaping with a nested QoS feature allows various congestion-based QoS features to work properly on the SVI.

Table 12-2 represents the corresponding Modular QoS CLI (MQC)–based features. In all cases, congestion is needed for the QoS feature to be activated.

Table 12-2 MQC–Based Features

Feature	Original Interface–Based QoS	Comparable MQC–Based QoS for the SVI
WRED, RED, DiffServ and Precedence Based	interface FastEthernet 0/0 random-detect	Class Based Traffic Shaping with Nested WRED
WFQ, CBWFQ	interface FastEthernet 0/0 fair-queue	Class Based Traffic Shaping with Nested WFQ/CBWFQ
LLQ	N/A	Class Based Traffic Shaping with Nested LLQ
Priority Queueing	interface FastEthernet 0/0 priority-group 2	Class Based Traffic Shaping with Nested LLQ
Custom Queueing	interface FastEthernet 0/0 custom-queue-list 1	Class Based Traffic Shaping with Nested CBWFQ

For example, configuring Low Latency Queuing (LLQ) and CBWFQ on the SVI supports shows a Class Based Traffic Shaping with Nested LLQ and CBWFQ QoS policy.

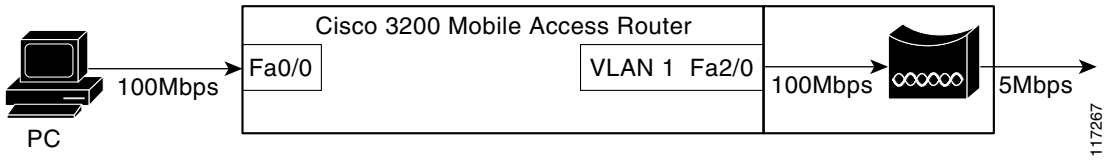
```
policy-map llq-cbwfq
 class voice
   priority percent 20
 class video
   bandwidth percent 20
 class data
bandwidth percent 60
! hierarchical(nested) policy map
policy-map traffic-shape-llq-cbwfq
  class ALL
    shape average 20000000
      service-policy llq-cbwfq
interface vlan 1
  service-policy output traffic-shape-llq-cbwfq
```

QoS on a Wireless Device

For a complete description of the QoS for Virtual Private Network (VPN) commands in this chapter, refer to the *Cisco IOS Quality of Service Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Figure 12-1 is an example of a configuration that requires QOS to be applied at the Fast Ethernet VLAN interface.

Figure 12-1 QOS Fast Ethernet VLAN Interface Scenario



The Fast Ethernet port of the router is connected to the wireless device by using a 100 Mbps link. The wireless device connects to the Internet through a 5 Mbps link. In this scenario, it is possible for the router to send traffic to the wireless device at 100 Mbps. The upstream bandwidth for the bridge is only 5 Mbps, and the packets that exceed this rate are dropped randomly by the bridge. If QoS policies are applied to the 10/100 Fast Ethernet 2/0 (VLAN 1) router port, you can control how the different kinds of traffic is handled, reducing the random packet drops and delays by the wireless device.

Class-Based Traffic Shaping

Class Based Traffic Shaping with Hierarchical Policy Maps shapes the packets sent out of an interface and applies QOS when traffic exceeds the shaping limit.

The general packet flow when Class Based Traffic Shaping along with Hierarchical Policy Maps is configured is as follows:

- A packet comes into an input interface.
- The output interface for the packet is identified.
- The packet is checked at the output interface to see if it falls within the shaping limit meant for that traffic-class. If so, the packet is transmitted, and the metrics updated accordingly. Otherwise, the packet is queued on to the output queue of the traffic-class, and the shaping-timer for that class is started.

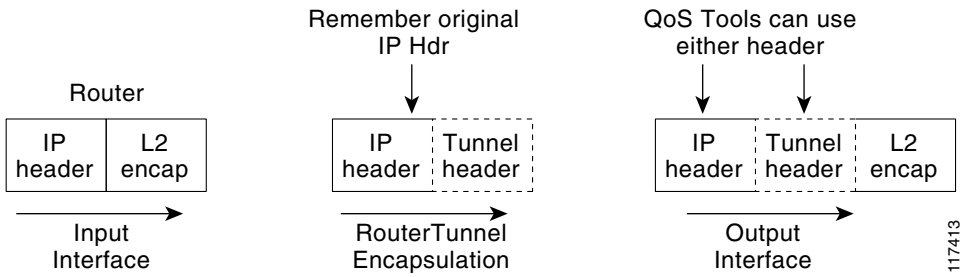
Older QOS policies like Priority Queuing and Custom Queueing are applied while en-queuing and de-queuing the packets from the output queues. When Modular QoS CLI (MQC) Traffic Shaping is used to achieve QOS, the 10/100 Fast Ethernet physical interface need not get congested; when the input rate reaches above the configured traffic shaping rate, QoS features such as Low Latency Queuing (LLQ) and Class-based Weighted Fair Queueing (CBWFQ) become active. Refer to the "QoS Restrictions" section for additional information.

After the packets have left the traffic shaping Fast Ethernet interface, they arrive at the WMIC Fast Ethernet interface. The WMIC can also provide QoS to the pre-marked priority traffic by providing radio prioritization.

How Mobile IP Interacts with QoS

By default, Mobile IP maintains the Type of Service (ToS) byte in the IP header. In Mobile IP, the router copies the TOS (QoS) bits that are in the original IP header into the new mobile IP tunnel header before forwarding the packet to the router.

Figure 12-2 Tunnel Encapsulation



This allows the QoS is configured on the home agent and transit routers to act on the packet based on these flags.

QoS for Mobile IP tunneled packets are affected as follows:

- Tunneled packets hide original data packets by encapsulation and could defeat QoS flow features
- Transit router policers do not see the original packet and might change the TOS bits in transit
- The QoS configuration on transit routers, including foreign agents, affects the tunneled packets

Mobile IP encapsulates the original packet for forwarding to the current location of the mobile access router. Therefore, transit routers making QoS decisions evaluate the new mobile IP tunnel IP header, not the original packet header.

Mobile IP tunnel headers (as do other types of tunnel headers, such as GRE, IPSec, and so forth) present some problems to policer statements on transit routers. Assume the network administrator has assigned all voice traffic received by the router a higher priority than data traffic and the TOS bits are changed to reflect that priority. When the packet arrives at the home agent and the Mobile IP tunnel interface receives the voice packet, the TOS bits are copied into the new IP header before being forwarded to the mobile access router. Unfortunately, the transit routers might not interpret the packets as containing voice, but instead consider them as IP-in-IP packets with an unauthorized TOS level and modify the TOS bits, affecting the QoS.

This leads to another problem for the home agent. When the home agent encapsulates the original packet, it loses the information it needs to properly do QoS features that require flow information on the outbound interface.

For QoS on the outbound interface of the home agent, there is a solution to this problem. By applying *qos-preclassify* on the tunnel interface template, the eventual outbound interface is able to apply QoS based on the original packet. For Mobile IP headers, the router remembers where the original header is located, so QoS processing can be done at the outbound interface.

If the packet destined for the mobile access router is inbound to a foreign agent, whatever QoS parameters are configured on that foreign agent router are applied to the packet, and the same problem is created; the packet is no longer recognized as a voice packet.

The Tunnel Template and Mobile IP

Typically, when you want to offer an interface-level service or add functionality to the interface, you add a command to the interface. Adding commands to a Mobile IP interface was previously impossible because the Mobile IP tunnel interfaces are dynamically generated. The tunnel template allows you to add features to the dynamic tunnels created by Mobile IP. This template can be applied to the dynamically-generated tunnels between the home agent and foreign agents, and the dynamically generated tunnels between the home agent and mobile access routers.

The two most relevant features applied to the dynamically generated tunnels are QoS pre classification and multicast PIM sparse mode. By applying *qos-preclassify* to the tunnel template, the original packet header is used to classify the packet on the outbound interface using information in the original IP header instead of the Mobile IP tunnel header. This allows Qos features, such as Weighted Fair Queuing (WFQ), to see different flows at the outbound interface.

By applying the *ip pim sparse mode* parameter to the tunnel template, the router can to send PIM join messages back to the home agent through the mobile access router home agent tunnel (with reverse tunnel enabled).

The following example shows the configuration of tunnel template on the mobile access router:

```
interface Tunnel50
 no ip address
! Allow PIM join messages to use tunnel
 ip pim sparse-mode
! Turn on Qos Pre-Classification
 qos pre-classify
!
!
ip mobile router
! Mobile Router Home Address
 address 65.1.1.1 255.255.255.0
```

```
! Home Agent
 home-agent 171.69.68.34
! Tunnel template to use for Mobile IP Tunnels
 template Tunnel50
! Turn on Reverse Tunnel. This allows the MR to send the multicast join messages directly
to the Home Agent
reverse-tunnel
```

The following example shows the configuration of the tunnel template on the home agent:

```
interface Tunnel100
 no ip address
! Allow PIM join messages to use tunnel
 ip pim sparse-mode
! Turn on Qos Pre-Classification
 qos pre-classify
!
!
! Define mobile node 65.1.1.1 as a mobile router
ip mobile mobile-networks 65.1.1.1
 description Chamber Automobile
! Tell Home Agent which mobile network this mobile router has
 network 172.21.58.0 255.255.255.0
! Define the template to use when creating a tunnel to the mobile router
 template Tunnel100
```

QoS Components Used with Mobile IP

The QoS components used with Mobile IP are:

- Class Map
- Policy Map
- Service Policy

Class Map

Class maps identify interesting traffic by using access control lists (ACLs). Another method of finding interesting traffic is to match the protocol, such as RTP. A third way to find interesting traffic is to match the Differentiated Services Code Point (DSCP) field. The first two class maps match the audio and video traffic based on the protocol. The third example uses an ACL to match the Registration Request (RRQ) Packet traffic.

```
class-map match-all video-in
  match protocol rtp video
class-map match-all voice-in
  match protocol rtp audio
class-map match-all rrq
  match access-group 101
!
access-list 101 permit udp any any eq mobile-ip
```

Policy Map

Policy maps use class maps to define the interesting traffic and to define what to do once the traffic is identified. The first policy map in this example, *inbound-marking*, changes the DSCP field of the packet and marks it as EF if it is a voice packet or AF41 if it is a video packet.

The second policy map, *low-latency-queue*, defines the percentage of bandwidth each class should have on the outgoing link. In class rrq, we are using a definitive percentage of the bandwidth. For example, it will always get 2 percent of the bandwidth as if it were a virtual link with that bandwidth. For class video, we specify a percentage of the remaining bandwidth after the definitive bandwidths are defined.

```
policy-map inbound-marking
  class voice-in
   set ip dscp ef
  class video-in
   set ip dscp af41
!
policy-map low-latency-queue
  class rrq
    priority percent 2
  class voice
    priority percent 50
  class video
   bandwidth remaining percent 70
  class highdata
   bandwidth remaining percent 30
  class class-default
   fair-queue
class-map match-all ALL
 match any
!
policy-map Shape20mbps
 class ALL
  shape average 20000000
  ! Nesting LLQ policy under traffic shaping
  service-policy low-lat-queue
```

Service Policy

The service-policy command applies the policy maps to the interfaces. In this example, the policy map, *inbound-marking*, is being applied to all traffic arriving on this interface. Just like ACLs are applied to inbound or outbound traffic, so can policy maps.

```
interface FastEthernet1/0
 ip address 172.69.4.1 255.255.255.0
 speed auto
 full-duplex
 service-policy input inbound-marking
interface vlan 1
 ! To workgroup bride
 service-policy output Shape20Mbps
```

qos pre-classify Command

Some QoS features require information typically found in the IP header to function correctly. The problem is tunnel encapsulation hides the original IP header. Without the **qos pre-classify** command, packets traversing across the same tunnel have the same tunnel header. If there is congestion on the interface, the packets are treated the same. When the **qos pre-classify** command is added to the tunnel template and the tunnel template is applied to the Mobile IP tunnel where the tunnel header is added to the packet, the router can correctly identify the classification of the packet.

The **qos pre-classify** command behaves differently for different encapsulation headers. For non-encryption headers, for example Mobile IP headers, the router identifies the location of the beginning of the original IP header and uses the original classification during QoS processing. For encryption type headers, the router takes a snapshot of the first 64 bytes of the packet, and QoS processing is performed at the outbound interface based on the snapshot. This command is restricted to tunnel interfaces, virtual templates, and crypto maps.

For example, flow-based Weighted Fair Queuing (WFQ) classifies all packets traversing a tunnel as a single WFQ flow, even though the packets might belong to different flows with different IP source and destination addresses, source and destination ports, and so forth. By using the **qos pre-classify** command, the location of the QoS information in the original IP header is identified for use on the outbound interface where the QoS features that balance the traffic flows are configured.

Table 12-3 illustrates the behavior of the QOS features when pre-classification is applied. Pre-classification does not affect queuing based on other information, such as the Differentiated Services Code Point (DSCP) value.

Table 12-3 Pre-classification Descriptions

QoS Feature	Description
WFQ, flow RED	Classify flows before tunnel encapsulation, each flow within a tunnel gets a fair share of the output interface bandwidth.
WRED	Identify IP precedence on pre-tunnel packet header (also achieved by the TOS byte copying by tunneling features).
PriorityQ, CustomQ	Classify packets before tunnel encapsulation or ACL matches on pre-tunnel packet header.
GTS	Classify flows before tunnel encapsulation within a shape queue for group-based GTS, ACL matches on pre-tunneled packet header.
FRTS	Classify flows before tunnel encapsulation within a shape queue, ACL matches on pre-tunneled packet header if PQ/CQ is configured.
CAR	ACL matches on pre-tunneled packet header. The set precedence DSCP action applies to outer IP header only.
CBWFQ, per-VC CBWFQ	Allow a class to match on pre-tunnel packet header. Classify flows before tunnel encapsulation for the class is the default.

Pre-classification Limitations

When a packet is fragmented after it has been tunnel-encapsulated (by GRE, L2TP, or IPnIP), all fragments are pre-classified by the output QOS features. However, pre-classification does not work on IP fragments that are encrypted. All fragments are classified based on the outer IPSec header only.

qos pre-classify Command

The **qos pre-classify** command can only be applied to a tunnel interface, virtual template interface, or crypto map configuration. The command syntax for Tunnel Interface configuration mode or crypto map configuration mode:

```
[no] qos pre-classify
```

For GRE/IPIP tunnels, the CLI is applied on the tunnel interface. That means pre-classification can be configured on a per-tunnel basis.

For L2F/L2TP tunnels, the CLI is applied on the virtual-template interface. Every L2TP client belonging to the same VPDN group inherits the pre-classification setting. The command can be configured on a per-VPDN tunnel basis.

For IPSEC tunnels, the CLI is applied on the crypto map, allowing configuration on a per-tunnel basis. QOS features on the physical interface that carries the crypto map can classify packets prior to encryption.

WMIC QoS Configuration

After the router shapes the outgoing traffic, the packets are forwarded to the WMIC. To provide radio prioritization on the WMIC, the following commands classify the incoming marked packets and prioritizes them on the radio interface:

```
class-map match-all voice-in
match ip dscp ef <?xml:namespace prefix = o ns = "urn:schemas-microsoft-com:office:office"
/>
class-map match-all video-in
match ip dscp 41
!
policy-map WirelessQoS
class voice-in
set cos 6
class video-in
set cos 4
interface Dot11Radio0
!
service-policy output WirelessQoS
```

Configuring QoS for VPNs

The QoS for VPNs feature, which is enabled by the **qos pre-classify** command, is restricted to tunnel and virtual template interfaces and crypto map configuration submodes.

For generic routing encapsulation (GRE) and IP in IP (IPIP) tunnel protocols, the **qos pre-classify** command is applied on the tunnel interface, making QoS for VPNs a configuration option on a per-tunnel basis.

For Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) protocols, the **qos pre-classify** command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the pre-classification setting. The **qos pre-classify** command can be configured on a per-VPDN tunnel basis.

For IPSec tunnels, the **qos pre-classify** command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.

To configure the QoS for VPNs feature on a tunnel or virtual interface basis, use the following commands, beginning in global interface mode:

	Command	Purpose
Step 1	`Router(config)# interface [tunnel-name | virtual-template-name]`	Enters interface configuration mode and specifies the tunnel or virtual interface to configure.
Step 2	`Router(config-if)# qos pre-classify`	Enables the QoS for VPNs feature.

To configure the QoS for VPNs feature on the crypto map configuration basis, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto map [map-name]`	Enters crypto map configuration mode and specifies the previously defined crypto map to configure.
Step 2	`Router(config-if)# qos pre-classify`	Enables the QoS for VPNs feature.

Example of QoS Configuration

The example configuration shows the tunnel template. The configuration is required only on mobile routers:

```
config t
int tunnel100 <- or any number
< any command defined inside the tunnel will be an inheritance to the mobile tunnel.>
qos pre-classify
exit
ip mobile router
template tunnel 100
```

The **shut** command is executed, and then the **no shut** command is executed on the roaming interface to implement the settings. To verify the configuration, use the **show ip mobile tunnel** command. The following example shows the tunnel template information.

```
Router#sh ip mobile tunnel
Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 5.0.0.3, dest 5.0.0.2
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Serial1/0.1
    MRcreated, fast switching enabled, ICMP unreachable enabled
    10 packets input, 1000 bytes, 0 drops
    59 packets output, 7906 bytes
```

```
Running template configuration for this tunnel:
qos pre-classify
ip rsvp bandwidth 100 100
```

Verifying QoS for VPNs

Use the **show interfaces** or **show crypto-map** command to verify that the QoS for VPNs feature has been successfully enabled on your router.

Note The **show queue** command output displays packet information, including whether the packet is previously classified. In a congested environment, using the **show queue** command might be useful for evaluating the environment and reconfiguring your router.

Verifying QoS for VPNs with the show interfaces Command

To verify that the QoS for VPNs feature has been successfully enabled on an interface, use the **show interfaces** command. The last line in the output (which is italicized for emphasis in the example) verifies that the QoS for VPNs feature is successfully enabled.

```
Queuing Strategy: fifo (QOS pre-classification)

Router# show interfaces

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Interface is unnumbered. Using address of Ethernet 3/2 (13.0.0.2)
MTU 1476 bytes, BW 9 Kbit, DLY 500000usec,
reliability 255/255. txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec)
Tunnel source 13.0.0.2 (Ethernet 3/2), destination 13.0.0.1
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Checksumming of packets disabled, fast tunneling enabled
Last input never, output 00:07:29, output hang never
Last clearing of "show interface" counters 1d05h
Queuing Strategy: fifo (QOS pre-classification)
```

Verifying QoS for VPNs with the show crypto map Command

To verify that the QoS for VPNs feature has been successfully enabled on a crypto map, use the **show crypto map** command. The last line in the output (which is italicized for emphasis in the example) verifies that the QoS for VPNs feature is successfully enabled.

```
Router# show crypto map

Crypto Map "testtag" 10 ipsec-isakmp
Peer = 13.0.0.1
Extended IP access list 102
access-list 102 permit gre host 13.0.0.2 host 13.0.0.1
Current peer:13.0.0.1
Security association lifetime: 4608000 kilobytes/86400 seconds
PFS (Y/N): N
Transform sets={proposal1,}
qos pre-classification
```

Monitoring and Maintaining QoS for VPNs

To monitor and maintain the QoS for VPNs feature, use the following commands in user EXEC mode, as needed:

Command	Purpose
`Router# show interfaces [tunnel-name | virtual-template-name]`	Displays information about the tunnel or the virtual template, including the queueing strategy.
`Router# show crypto map [map-name]`	Displays information about the crypto map. If the QoS for VPNs feature is enabled, a **qos pre-classification** line appears in the command output.

Examples of QoS for VPNs Configuration

This section provides QoS for VPNs configuration examples. For additional information on how to configure QoS for VPNs, see the section "Configuring QoS for VPNs" in this chapter.

Example of Configuring QoS for VPNs for GRE and IPIP Tunnel Protocols

In the following example, *tunnel0* is the tunnel name. The **qos pre-classify** command enables the QoS for VPNs feature on tunnel0.

```
Router(config)# interface tunnel0
Router(config-if)# qos pre-classify
```

Example of Configuring QoS for VPNs for L2F and L2TP Tunnel Protocols

In the following example, virtual-template1 is the virtual-template name. The **qos pre-classify** command enables the QoS for VPNs feature on virtual-template1.

```
Router(config)# interface virtual-template1
Router(config-if)# qos pre-classify
```

Example of Configuring QoS for VPNs for IPSec Tunnel Protocols

In the following example, secured-partner-X is the crypto map name. The **qos pre-classify** command enables the QoS for VPNs feature on secured-partner-X.

```
Router(config)# crypto map secured-partner-X
Router(config-crypto-map)# qos pre-classify
```

Traffic Shaping in a Wireless Environment

In typical scenario, the wireless device is connected internally to a Fast Ethernet port on the FESMIC to provide roaming capability. A wireless workgroup bridge has lower bandwidth than the Fast Ethernet port on the FESMIC. A heavy burst of traffic can cause packets to be dropped by the wireless device. It is necessary to shape the packets being sent out of the FESMIC Ethernet interface at rate that corresponds to uplink speed of the wireless device.

The packets are classified into different flows so each flow can be handled in accordance with the desired QoS parameters by using Class Based Traffic Shaping with Hierarchical Policy Maps.

For a brief description of how to configure QOS using Class Based Traffic Shaping along with Hierarchical Policy Maps, see "Class-Based Shaping" at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt4/qcfpolsh.htm.

Using access control lists for classifying the packets into various classes is not recommended as this results in the throttling of the input interface even at low loads. It is recommended that you use a separate device to classify the packets and do the marking so that the router can then classify the packets based on IP precedence by using the **match ip precedence** <*precedence value*> command.

Note When a router is mobile, there is no mechanism in the wireless device or in the router to have traffic shaping reconfigure the traffic shaping rate. The traffic shaping rate should be set to the average bandwidth available to the router in the wireless coverage area.

Related Documentation

For additional configuration information on the WMIC, see "Cisco 3200 Series Wireless MIC Software Configuration Guide."

For introductory QoS information:

- http://www.cisco.com/go/qos
- http://www.cisco.com/warp/public/105/qostunnel.html
- http://www.cisco.com/warp/public/105/crypto_qos.html

Configuring QoS for VPNs:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfvpn.htm

12.2 QoS Configuration Guide:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

12.2 QoS Command Reference Guide:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/index.htm

Cisco AVVID Network Infrastructure Enterprise QoS Design Guide:
http://www.cisco.com/warp/customer/771/srnd/qos_srnd.pdf

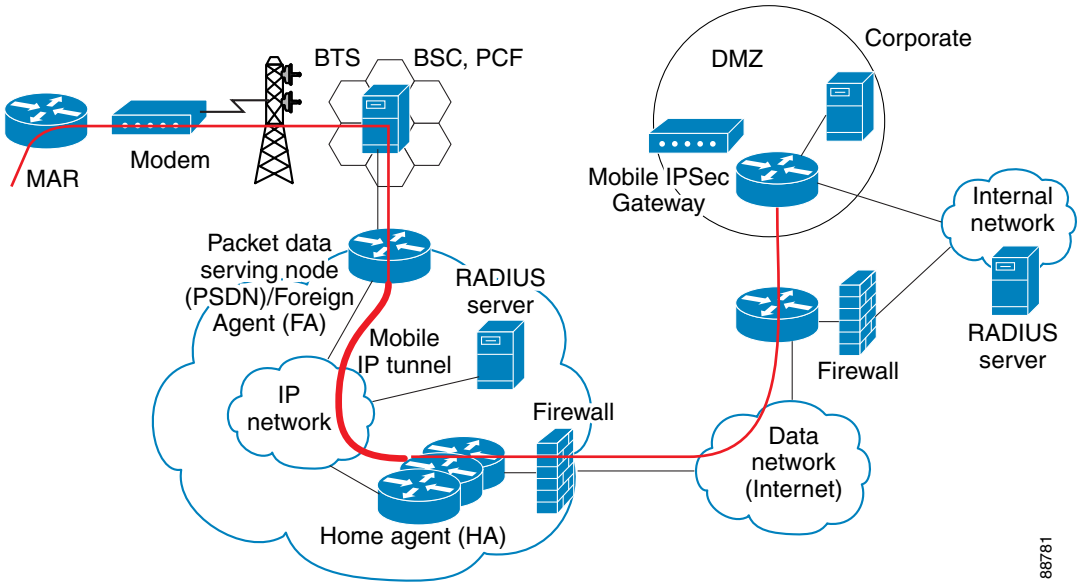
Modems in a Mobile Environment

This chapter describes roaming with external wireless modems.

Roaming with External Wireless Modems

General Packed Radio Service/Code Division Multiplex Access (GPRS/CDMA) modems provide the mobile access router with a Layer 2 roaming interface. The Mobile IP stack allows layer 3 roaming IP connectivity for the mobile access router. External modems are connected to a serial interface of the mobile access router. The serial interface should be running in asynchronous mode. Figure 13-1 shows a sample scenario in which the serial port of the mobile access router is connected to a CDMA modem.

Figure 13-1 Modem to Mobile Access Router Connection



The mobile access router supports the following modems:

- Airlink Raven
- AnyDATA I-Port
- Wavecom

Configuration Example

The example configurations shown in Figure 13-2 and Figure 13-3 demonstrate the router's ability to roam back and forth between 802.11b and Cellular technologies. The browser-based applications and video move dynamically to and from the different technologies. The 1X technology provides approximately 60 Kbps. The Nextel provides approximately 20 Kbps, but the network provides for static IP addresses and private links back to the headquarters. Implementing IPsec VPN in the mobile access router provides a secure connection back to the headquarters through 802.11b technology.

Figure 13-2 IPsec VPN Connection

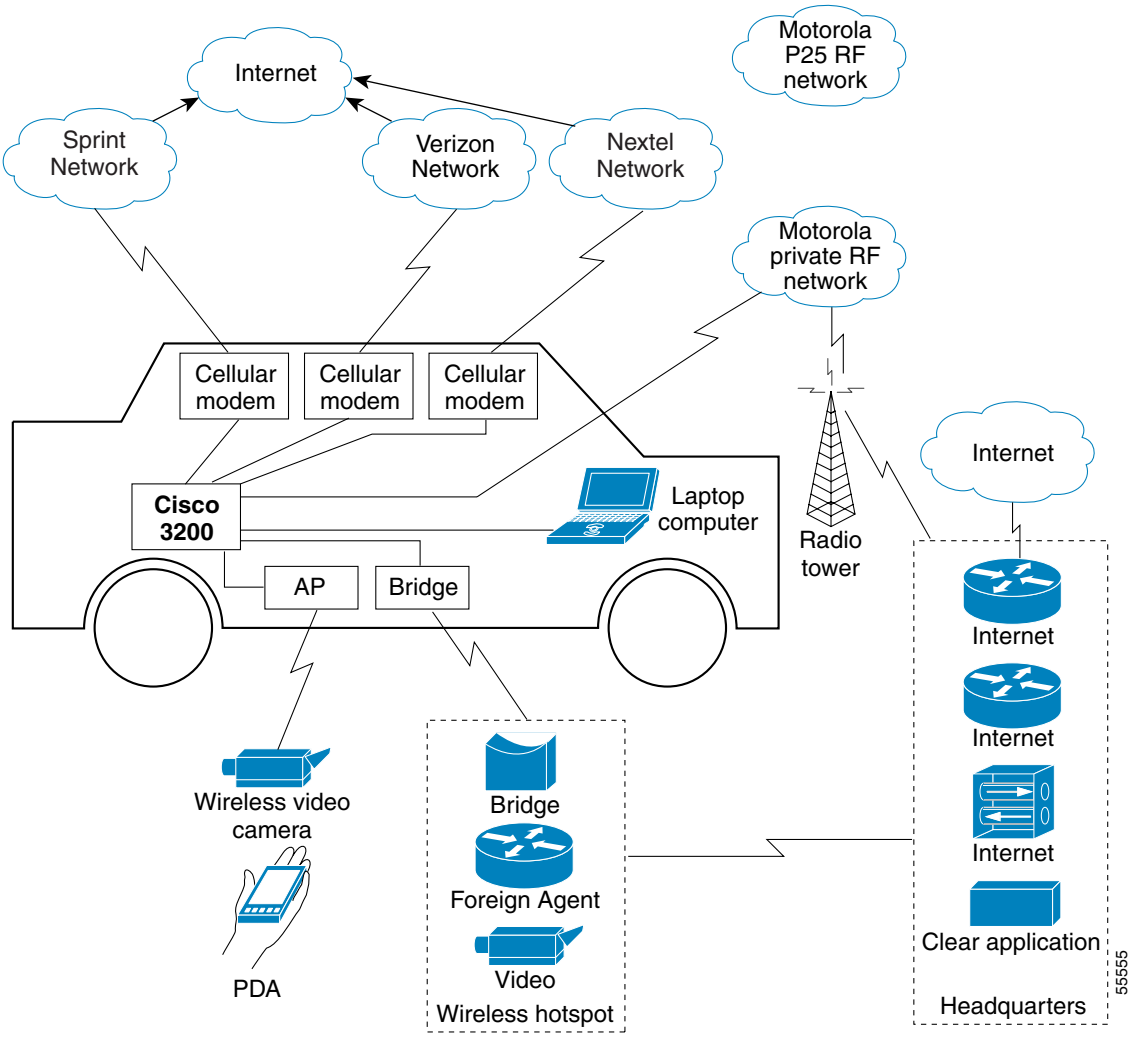
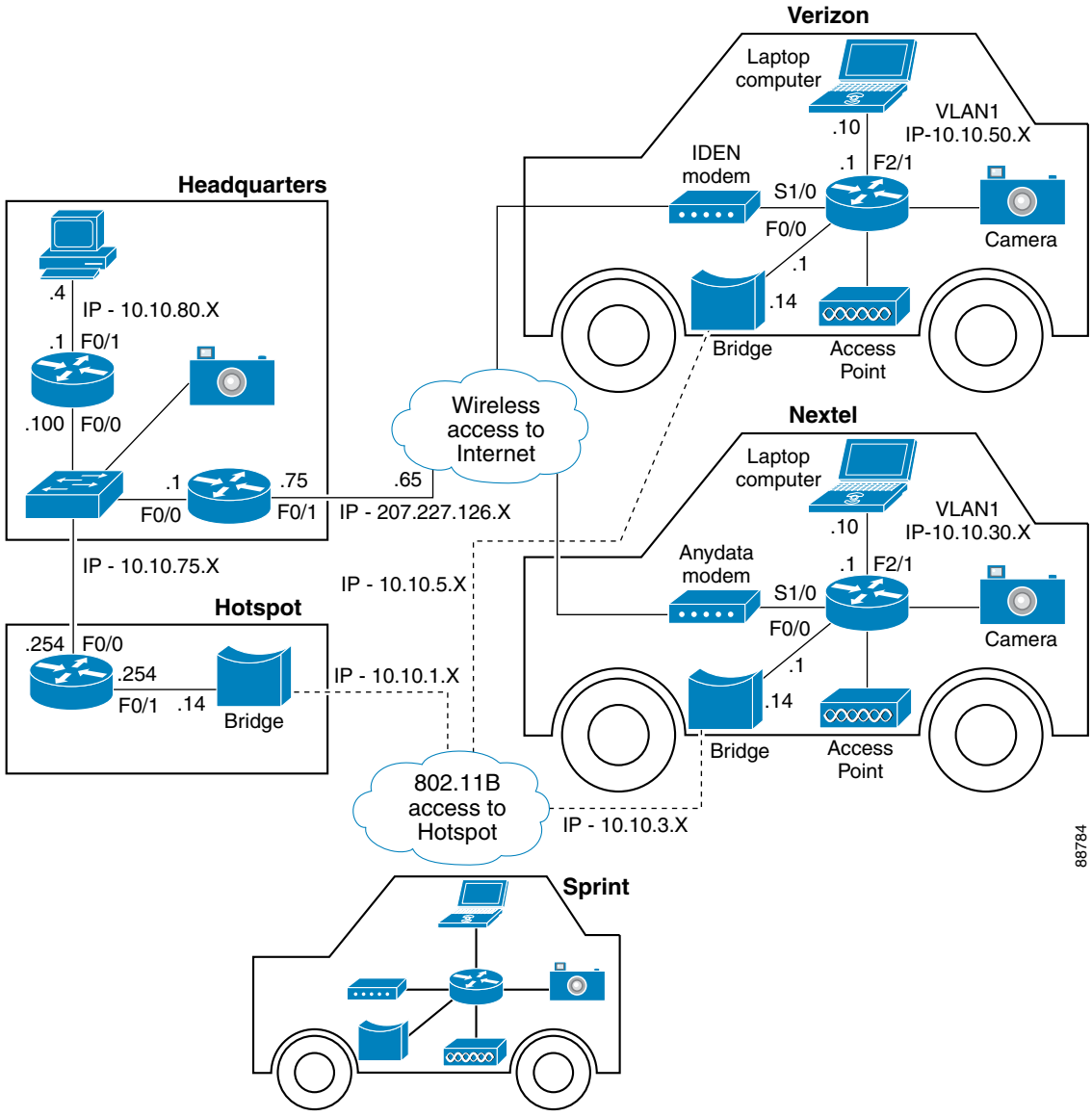


Figure 13-3 Wireless Internet Connection



Example of a Mobile Access Router with Dialer Interface and GRE Mobile IP Tunneling

```
chat-script airlink-cdma "" "AT&C1&D2" TIMEOUT 30 OK "ATDT#19788" TIMEOUT 30 CONNECT
!
interface Loopback0
 ip address 15.4.1.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.20.1.1 255.255.255.0
!
```

```
interface Serial1/0
 physical-layer async
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 dialer-group 1
!
interface Dialer0
 ip address negotiated
 ip nat outside
 ip mobile router-service roam
 ip mobile router-service collocated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string 1
 dialer persistent
 dialer-group 1
!
ip mobile secure home-agent 64.161.107.162 spi 100 key hex
12345678123456781234567812345678 algorithm md5 mode prefix-suffix
ip mobile router
 address 15.4.1.2 255.255.255.0
 home-agent 64.161.107.162
 reverse-tunnel
 tunnel  mode  gre
!
line 1
 exec-timeout 0 5
 flush-at-activation
 script dialer airlink-cdma
 modem InOut
 no exec
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
 exec-timeout 0 0
 speed 115200
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
```

Example of a Mobile Access Router Without Dialer Interface

```
hostname 3200
!
chat-script airlink-cdma "" "AT&C1&D0" TIMEOUT 30 OK "ATDT#19788" TIMEOUT 30 CONNECT
!
interface Loopback0
 ip address 15.4.1.2 255.255.255.0
!
interface Serial1/0
 physical-layer async
 mtu 1450
 bandwidth 115200
 ip address negotiated
 ip mobile router-service roam
 ip mobile router-service collocated
```

```
 encapsulation ppp
 keepalive 900
 dialer in-band
 dialer idle-timeout 0
 dialer string airlink-cdma
 dialer-group 1
 async default routing
 async mode interactive
 no peer default ip address
 no fair-queue
 no ppp lcp fast-start
!
router mobile
!
ip mobile secure home-agent 64.161.107.162 spi 100 key hex
12345678123456781234567812345678 algorithm md5 mode prefix-suffix
ip mobile router
 address 15.4.1.2 255.255.255.0
 home-agent 64.161.107.162
!
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
!
line 1
 exec-timeout 0 0
 flush-at-activation
 script dialer airlink-cdma
 login
 modem InOut
 no exec
 transport input all
 autoselect during-login
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
!
line aux 0
 exec-timeout 0 0
 speed 115200
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
```

Example of a Mobile Access Router with Multiple Wireless Connections

```
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool testpool
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1 255.255.255.0
   dns-server 204.117.214.10
!
```

```
ip cef
chat-script airlink-cdma2 "" "ATDT#19788" TIMEOUT 60 "CONNECT"
chat-script tmobile "" "AT" TIMEOUT 5 OK "ATE0V1" TIMEOUT 5 OK "ATS0=0" TIMEOUT 5 OK
"AT+CGATT=1" TIMEOUT 5 OK "AT+CGACT=1,1" TIMEOUT 5 OK "ATD*99***1#" TIMEOUT  10 CONNECT
chat-script anydata "" "AT&C1&D0" TIMEOUT 30 OK "ATDT#777" TIMEOUT 30 CONNECT
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
!
interface Serial2/0
 physical-layer async
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 no keepalive
!
interface Serial2/1
 physical-layer async
 no ip address
 encapsulation ppp
 shutdown
 dialer in-band
 dialer pool-member 2
 no keepalive
!
interface Dialer0
 ip address negotiated
 ip mobile router-service roam priority 130
 ip mobile router-service collocated registration retry 3
 ip mobile router-service collocated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string 1
 dialer persistent
 dialer-group 1
 ppp authentication pap callin optional
!
interface Dialer1
 ip address negotiated
 ip mobile router-service roam
 ip mobile router-service collocated registration retry 3
 ip mobile router-service collocated
 encapsulation ppp
 dialer pool 2
 dialer idle-timeout 0
 dialer string 2
 dialer persistent
 dialer-group 2
 ppp chap hostname 4082029572
 ppp chap password 0 vzw
!
ip mobile secure home-agent 64.161.107.162 spi 100 key ascii hello algorithm md5 mode
prefix-suffix
ip mobile router
 address 20.20.20.1 255.255.255.0
 collocated single-tunnel
 home-agent 64.161.107.162
 mobile-network FastEthernet0/0
 reverse-tunnel
 tunnel mode gre
!
```

```
line 5
 exec-timeout 0 5
 flush-at-activation
 script dialer airlink-cdma2
 modem InOut
 no exec
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line 6
 exec-timeout 0 5
 flush-at-activation
 script dialer anydata
 modem InOut
 no exec
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
```

Example of a Home Agent Configuration

```
hostname HomeAgent
!
ip subnet-zero
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 10.10.100.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 64.161.107.162 255.255.255.248
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 64.161.107.161
ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile virtual-network 15.4.0.0 255.255.0.0
ip mobile host 15.4.1.2 virtual-network 15.4.0.0 255.255.0.0
ip mobile secure host 15.4.1.2 spi 100 key hex 12345678123456781234567812345678
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
```

Initialization Strings

Recommended initialization strings for some common modems are provided in Table 13-1, but be aware that Cisco does not warrant that they are suitable or current. When in doubt, refer to the modem vendor's documentation or technical support.

Table 13-1 Modem Chat Scripts

Modem	Network	Script
Airlink Raven	Sprint	chat-script airlink-cdma "" "ATDT#19788" TIMEOUT 60 "CONNECT"
Airlink Raven	Verizon	chat-script airlink-cdma "" "ATDT#19788" TIMEOUT 60 "CONNECT"
AnyDATA I-Port EMIII	Verizon	chat-script anydata "" "AT&C1&D0" TIMEOUT 30 OK "ATDT#777" TIMEOUT 30 CONNECT
Sony/Ericsson T68i Handset	AT&T	chat-script ericsson-gprs "" "AT" TIMEOUT 30 OK "ATE0Q0&C1&D2V1" TIMEOUT 60 OK "AT" TIMEOUT 30 OK "ATS0=0" TIMEOUT 30 OK "AT" TIMEOUT 30 OK "ATE0Q0&C1&D2V1" TIMEOUT 60 OK "AT" TIMEOUT 30 OK "ATDT*99***1#" TIMEOUT 30 CONNECT
Wavecom	T-Mobile or AT&T	chat-script tmobile "" "AT" TIMEOUT 5 OK "ATE0V1" TIMEOUT 5 OK "ATS0=0" TIMEOUT 5 OK "AT+CGATT=1" TIMEOUT 5 OK "AT+CGACT=1,1" TIMEOUT 5 OK "ATD*99***1#" TIMEOUT 10 CONNECT
Motorola i90c	Nextel	chat-script ModemTech "" "ATZ2" OK "AT&C1&D2" OK "ATDT" TIMEOUT 60 CONNECT

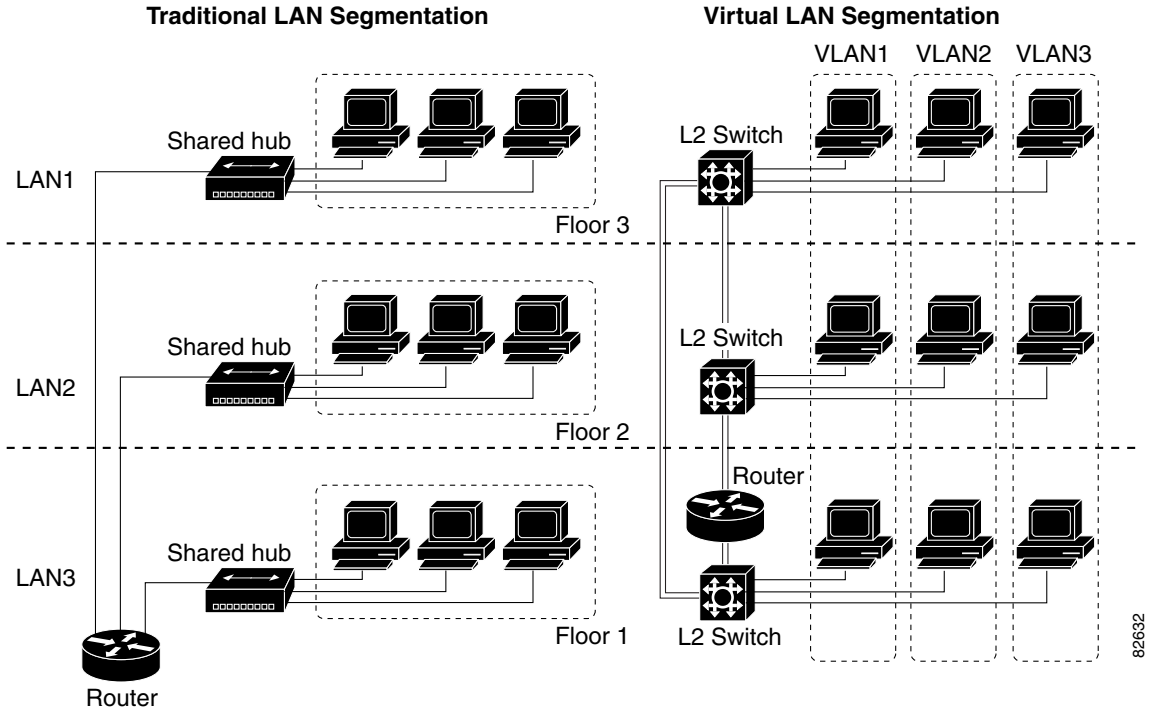
FESMIC Switch Port Functionality

The 10/100 Fast Ethernet ports on the FESMIC default to Layer 2 switch ports. The FESMIC is a "learning bridge," as defined in 802.1D with the Virtual Local Area Network (VLAN) capabilities of 802.1P/Q. The BCM5618 is fully capable of line-rate switching for all four 10/100 Fast Ethernet ports.

VLANs provide the segmentation services traditionally provided by routers in LAN configurations, as shown in Figure 14-1. VLANs make it easy to move an network or to change a network design.

- Broadcast control—Just as switches physically isolate collision domains for attached hosts and only forward traffic out a particular port, VLANs provide logical collision domains that confine broadcast and multicast traffic to the bridging domain.VLANs solve the scalability problems of large flat networks by breaking a single broadcast domain into several smaller broadcast domains.
- Security—VLANs improve security by isolating groups. High-security users can be grouped into a VLAN, possibly on the same physical segment. If you do not include a router in a VLAN, no one outside that VLAN can communicate with the users inside the VLAN and vice versa. This extreme level of security can be highly desirable. Users outside that VLAN cannot penetrate into the VLAN without an appropriate routing through secure Layer 3 routing services.
- Performance—Users that require high-performance networking can be assigned to their own VLAN. You might, for example, assign an engineer who is testing a multicast application and the servers that the engineer is using to a single VLAN. The engineer experiences improved network performance by being on a "dedicated LAN." The rest of the engineering group experiences improved network performance, because the traffic generated by the network-intensive application is isolated to another VLAN. This of course implies some areas of physical isolation of separate VLANs or prioritized service by tagging support and prioritized queuing classes within the switches and bridges of the 802.1Q VLAN.
- Network management—Software on the switch allows you to assign users to VLANs. Changing the cabling to change connectivity is no longer necessary in the switched LAN environment because network management tools allow you to reconfigure the LAN logically in seconds.

Figure 14-1 Traditional LAN Segmentation versus VLAN Segmentation



Port-Based VLAN

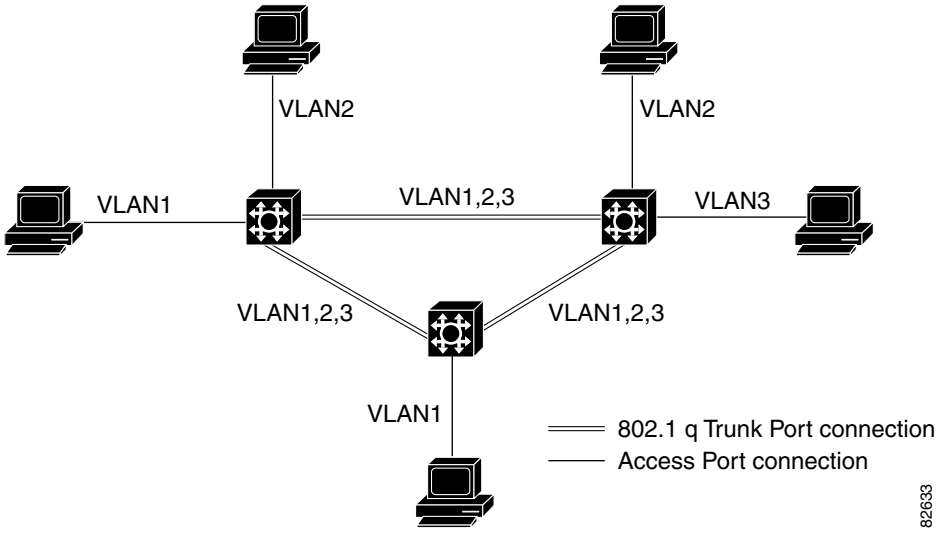
By default, the four 10/100 Fast Ethernet interfaces on the FESMIC are defaulted to Layer 2 switch ports and all four interfaces belong to VLAN 1. You can partition the switch ports to belong to different VLAN groups by using the **switchport vlan access** <*vlan-id*> command. The following is a brief function description of a FESMIC port-based VLAN:

- Each VLAN has its own MAC address table.
- Packets received are forwarded only to ports that are members of the same VLAN as the receiving port. VLAN partitions provide hard firewalls for all traffic in different VLANs.
- A VLAN comes into existence when a user adds a VLAN to the local VLAN database. A maximum of 32 VLANs are supported. VLAN IDs can range from 1 to 1005.
- By default, a spanning tree instance is created for each VLAN.

802.1Q Trunking

A trunk is a point-to-point link between one or more Ethernet switch ports and another networking device, such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link, and they allow you to extend VLANs across an entire network, as shown in Figure 14-2. The IEEE 802.1q protocol is an industry-standard trunking encapsulation.

Figure 14-2 802.1Q Trunk Port Application

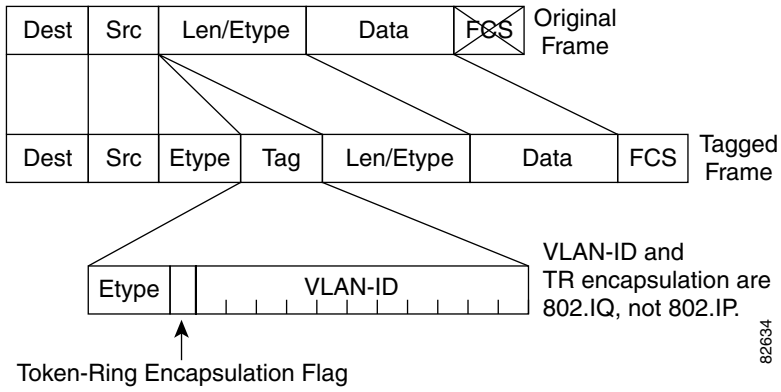


The 802.1Q trunk port is used for VLAN extension from one switch to another 802.1Q-capable switch, and used for an 802.1Q-capable router for inter-VLAN routing. The FESMIC supports both the VLAN extension and inter-VLAN routing.

The 802.1Q uses an internal tagging mechanism. Internal tagging means that a tag is inserted within the frame. Note that on an 802.1Q trunk, one VLAN is *not* tagged. This VLAN, named the *native VLAN*, must be configured the same on each side of the trunk. We can deduce to which VLAN a frame belongs when we receive a frame with no tag. The EtherType field identifying the 802.1Q frame is 0x8100. In addition to the 12-bit VLAN-ID, 3 bits are reserved for 802.1P priority tagging, as shown in Figure 14-3. Also, note that inserting a tag into a frame that already has the maximum Ethernet size creates a 1522 byte frame, that can be considered a “baby giant” by the receiving equipment.

The FESMIC is capable of 802.1Q tagging, only supporting 802.1Q trunking encapsulation. It does not support the Cisco proprietary ISL encapsulation.

Figure 14-3 802.1Q Tag Format in an Ethernet Frame

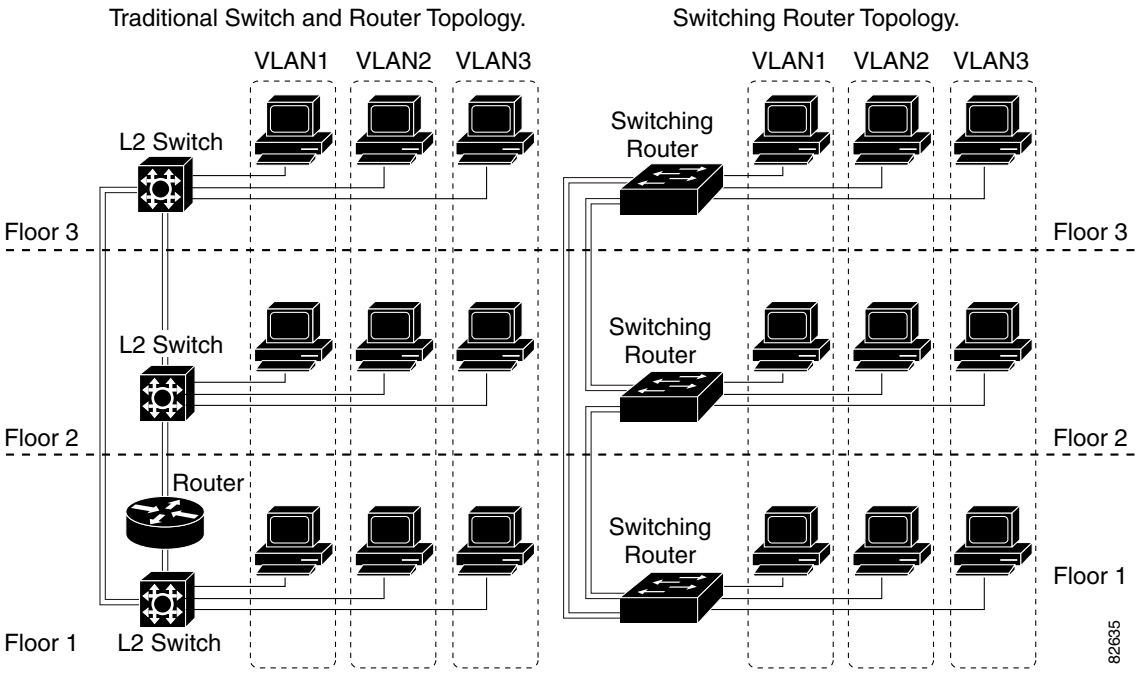


Inter-VLAN Routing

In a VLAN network, traffic and stations for multiple network layer subnets (VLANs) can coexist on a single physical LAN segment. In practice, a single VLAN corresponds to a network subnet, and a VLAN trunking capable router is required to forward traffic from a first VLAN to a second VLAN for a Layer 2 switch.

The FESMIC enables the Cisco 3200 Series router to become one of first IOS Ethernet switching routers to deliver intelligent Layer 2 switching capability and Layer 3 inter-VLAN routing in a single box solution, as shown in Figure 14-4

Figure 14-4 Switching Router Network Topology



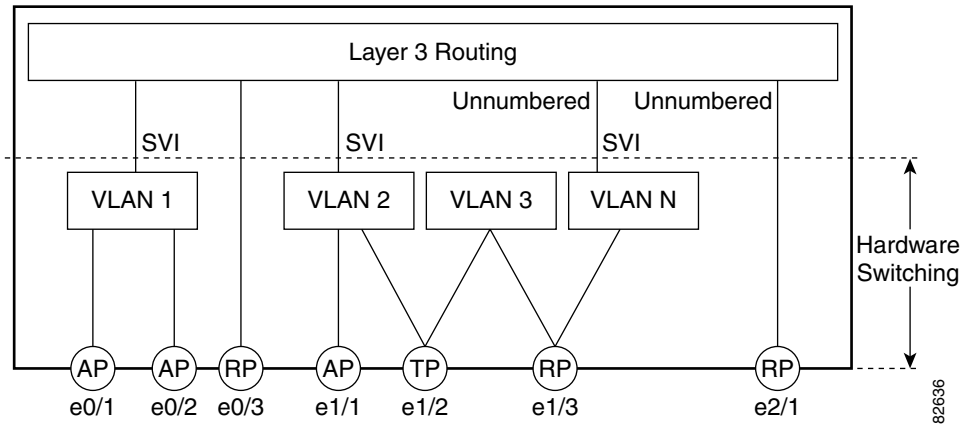
In a typical IOS-managed Layer 2 switch, there would be one Layer 3 Switch Virtual Interface (SVI) that allows you to configure the device over a Layer 3 protocol by using SNMP or a Telnet application. This is referred to as the *management VLAN* for the switch. The default management VLAN is usually the native VLAN 1. The configurable VLAN device allows you to configure any VLAN to be the management VLAN, but there can be only one virtual Layer 3 interface in one VLAN.

A switch routing module, like the FESMIC, allows you to use the SVI to configure more than one virtual Layer 3 interface to support routing between the different VLANs, and the virtual Layer 3 interface of any other router interface in the system, as shown in Figure 14-5.

You can manage the switching router with any switch virtual Layer 3 interface created in the system. The FESMIC router switch port is an interface capable of handling Layer 3 switching functionality in hardware. The SVI architecture has the framework to support such a functionality.

- A SVI represents a VLAN of switch ports as one interface to the routing function in the system.
- There is at most one SVI associated with a VLAN.
- It is not necessary to configure an SVI for every known VLAN. It is only necessary to configure a SVI when you want to route between VLANs or want to provide IP host connectivity to the rest of the network by using any of the mobile access router routed interfaces.
- One management SVI, interface VLAN 1, is created at system initialization to permit remote administration. Additional SVIs exist only when explicitly configured by a user.

Figure 14-5 Switch Virtual Interface Architecture



VLAN Trunk Protocol (VTP)

VLAN Trunk Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a *VLAN management domain*) is made up of one or more switches that share the same VTP domain name and that are interconnected with trunks. VTP minimizes configuration errors and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

The FESMIC supports both VTP version 1 and version 2.

- VTP server mode—You can create, modify, or delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches, based on advertisements received over trunk links. VTP server is the default mode.
- VTP clients mode— Behaves the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- VTP transparent mode—Switches do not participate in VTP. A VTP-transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk interfaces.

VTP Server Example

The following example shows how to configure the switch as a VTP server:

```
Router# vlan database
Router(vlan)# vtp server
Setting device to VTP SERVER mode.
Router(vlan)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Router(vlan)# vtp password WATER
Setting device VLAN database password to WATER.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

VTP Client Example

The following example shows how to configure the switch as a VTP client:

```
Router# vlan database
Router(vlan)# vtp client
Setting device to VTP CLIENT mode.
Router(vlan)# exit

In CLIENT state, no apply attempted.
Exiting....
Router#
```

Disabling VTP (VTP Transparent Mode) Example

The following example shows how to configure the switch as VTP transparent:

```
Router# vlan database
Router(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

VTP Version 2 Example

The following example shows how to enable VTP version 2:

```
Router# vlan database
Router(vlan)# vtp v2-mode

V2 mode enabled.
Router(vlan)# exit

APPLY completed.
Exiting....
Router#
```

802.1P CoS

The IEEE 802.1P specification defines eight levels of priority (0 thru 7), with priority 7 being the highest priority. This information is carried in the 3-bit priority field of the VLAN tag header.

The FESMIC supports up to two class of service (CoS) queues per port. For the tagged packets, the incoming packet priority can be mapped into one of the queues, based on the priority field in the tag header or from the result of filtering mechanism. For untagged packets, the CoS priority is derived either from a programmable field within the ARL (MAC address table) or from the result of filtering mechanism.

After the packets are mapped into a CoS queue, they are forwarded or conditioned using these scheduling algorithms:

- Strict priority-based scheduling—Any packets residing in the higher priority queues are transmitted first. Only when these queues are empty will packets of lower priority be transmitted. The disadvantage of this scheme is the potential starvation of packets in lower priority queues.
- Weighted round-robin scheduling—This scheme alleviates the starvation of packets in lower priority queues by providing a certain minimum bandwidth to all queues for transmission. This bandwidth is programmable as the maximum number of packets of each CoS.

The FESMIC 10/100 Fast Ethernet interfaces default to use the strict priority-based scheduling. After system boots, you can enable weighted round-robin scheduling.

Mapping 802.1P priority to IP precedence bits is not supported.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between any two stations. When two ports on a switch are in a loop, the spanning tree port priority and port path cost setting determine which port to put in the forwarding state and which port to put in the blocking state.

The 802.1Q standard defines the method for running multiple VLANs over single or multiple physical LAN segments and defines a unique spanning tree instance to be created on each of the VLAN instances for all the VLANs in a network.

A mono spanning tree (MST) network lacks some flexibility, compared to a per VLAN spanning tree (PVST) network, which runs one instance of STP per VLAN. One spanning tree is created for every new VLAN created on a FESMIC interface. STP is enabled by default on VLAN 1 and on all newly created VLANs.

Cisco developed PVST+ to allow running several STP instances (even over an 802.1Q network) by using a tunneling mechanism. Although beyond the scope of this document, PVST+ can be briefly described as utilizing a Cisco device to connect a MST zone (typically another vendor's 802.1Q-based network) to a PVST zone (typically a Cisco 802.1Q-based network). There is no specific configuration to enter in order to achieve this. PVST+ is a spanning tree that allows the coexistence of both PVST and Shared Spanning Tree Protocol (SSTP) in a mixed vendor environment.

The STP described in IEEE 802.1D standard takes a substantial amount of time to converge to a loop free topology. It fails to take advantage of the point-to-point wiring found in modern networks. PVST is enabled on all switch platforms. Rapid Spanning Tree Protocol (RSTP), specified in IEEE 802.1w[9], improves the operation of STP, while maintaining compatibility with equipment based on the (original) 802.1d Spanning Tree standard.

Note The Cisco Shared Spanning Tree Architecture documents use the terms MST and SST to mean "Mono Spanning Tree" and "Shared Spanning Tree" respectively. The IEEE 802.1s[10] uses the same terms but with exactly opposite meanings, i.e. MST is "Multiple Spanning Trees" and SST is" Single Spanning Tree."

When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge packet data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP).

One spanning tree is created for every new VLAN that is created on the FESMIC. STP is enabled by default on VLAN 1 and on all the newly created VLANs.

PVST and PVST+ are enabled by default on the FESMIC.

For detailed information on how STP works, go to http://www.cisco.com.

Switch Virtual Interface

A Switch Virtual Interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. Only one SVI can be associated with a VLAN, but it is necessary to configure an SVI for a VLAN only when you wish to route between VLANs, fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured. In Layer 2 mode, SVIs provide IP host connectivity only to the system; in Layer 3 mode, you can configure routing across SVIs.

SVIs are created the first time that you enter the **vlan** interface configuration command on a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

SVIs support routing protocol and bridging configurations.

Creating a SVI

To make any of the 2-port FESMIC or the 4-port FESMIC switchports routable, do the following:

Step 1 Create a VLAN ID that will be used for the VLAN.

Step 2 From the enable prompt, (not the global configuration prompt) enter the following commands:

```
Router#vlan database
! your prompt is now "Router(vlan)#"
Router(vlan)#vlan 7
Router(vlan)#exit
```

Note If you skip Step 2, your switchport virtual interface line protocol will be down.

Step 3 Go to global configuration mode and enter your switchport.

```
Router>conf t
Router#interface FastEthernet3/0
Router(config-if)#switchport access vlan 7
```

Step 4 Configure the IP address for the interface by entering the SVI

```
Router(config-if)#interface configuration:
Router(config-if)#interface vlan 7
Router(config-if)#ip address 7.7.7.7 255.255.255.0
```

The 10/100 Fast Ethernet 3/0 switchport can be pinged by through the VLAN interface. You can now attach any Layer 3 features to interface with the VLAN.

IP Multicast Layer 3 Switching

This section describes how to configure IP multicast Layer 3 switching.

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

For complete information and procedures, refer to these publications:

- *Cisco IOS IP Configuration Guide*, Release 12.2, at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/
- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
- Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/index.htm
- Cisco IOS IP Command Reference, Volume 3 of 3: Routing Protocols, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprmc_r/index.htm

To enable IP multicast routing globally, Use this command in global configuration mode:

Command	Purpose
`Router(config)# ip multicast-routing`	Enables IP multicast routing globally.

Enabling IP PIM on Layer 3 Interfaces

You must enable PIM on the Layer 3 interfaces before IP multicast Layer 3 switching functions on those interfaces.

To enable IP PIM on a Layer 3 interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface vlan` *vlan_id* `{slot/port}`	Selects the interface to be configured.
Step 2	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	Enables IP PIM on a Layer 3 interface.

This example shows how to enable PIM on an interface using the default mode (**sparse-dense-mode**):

```
Router(config-if)# ip pim
Router(config-if)#
```

This example shows how to enable PIM sparse mode on an interface:

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#
```

Verifying IP Multicast Layer 3 Hardware Switching Summary

The **show ip pim interface count** command verifies the IP multicast Layer 3 switching enable state on IP PIM interfaces and the number of packets received and sent on the interface.

Note The **show interface statistics** command does not verify hardware-switched packets, only packets switched by software.

Use the following show commands to verify IP multicast Layer 3 switching information for an IP PIM Layer 3 interface, as illustrated below:

Step 1 Enter the **show ip pim interface count** command.

```
Router# show ip pim interface count

State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface          FS  Mpackets In/Out
10.15.1.20       GigabitEthernet4/8 * H 952/4237130770
10.20.1.7        GigabitEthernet4/9 * H 1385673757/34
10.25.1.7        GigabitEthernet4/10* H 0/34
10.11.1.30       FastEthernet6/26   * H 0/0
10.37.1.1        FastEthernet6/37   * H 0/0
1.22.33.44       FastEthernet6/47   * H 514/68
```

Step 2 Enter the **show ip mroute count** command.

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```

Note The -tive counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

Step 3 Enter the **show ip interface vlan 10** command.

```
Router# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.0.0.6/8
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.13 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
```

```
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
IP multicast multilayer switching is enabled
IP mls switching is enabled
Router#
```

Verifying the IP Multicast Routing Table

Use the **show ip mroute** command to verify the IP multicast routing table.

Step 1 Enter the **show ip mroute** command.

```
Router# show ip mroute 230.13.13.1

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
           Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:
 GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H
```

```
(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
 Outgoing interface list:Null
Router#
```

Note The RPF-MFD flag indicates that the flow is completely hardware switched. The H flag indicates that the flow is hardware-switched on the outgoing interface.

Storm Control

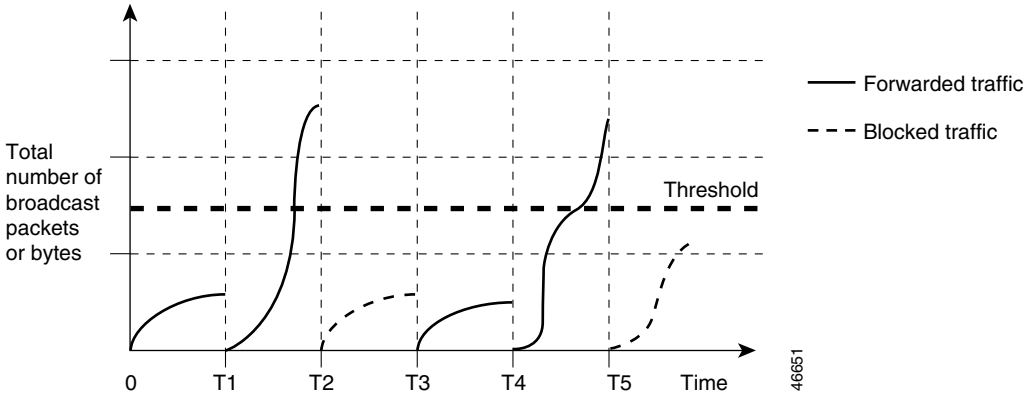
A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole, although it operates on a per-interface basis. By default, storm control is disabled.

Storm control prevents switch ports on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a storm.

Storm control monitors incoming traffic statistics over a time period and compares the measurement with a predefined suppression level threshold. The threshold represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

The graph in Figure 6 shows broadcast traffic patterns on an interface over a given period of time. In this example, the broadcast traffic exceeded the configured threshold between time intervals T1 and T2 and between intervals T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped. Therefore, broadcast traffic is blocked during those intervals. At the next time interval, if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 6 Broadcast Suppression Example



When storm control is enabled, the switch monitors the packets that are passing from an interface to the switching bus and determines whether the packet is unicast, multicast, or broadcast. The switch monitors the number of broadcast, multicast, or unicast packets received within the 1-second time interval, and

when a threshold for one type of traffic is reached, that type of traffic is dropped. This threshold is specified as a percentage of the total available bandwidth that can be used by broadcast (multicast or unicast) traffic.

The combination of broadcast suppression threshold numbers and the 1-second time interval control the way the suppression algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic.

Note Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

The switch continues to monitor traffic on the port. When the utilization level falls back below the threshold level, the type of traffic that was dropped is forwarded again.

Use the **storm-control broadcast**, **storm-control multicast**, and **storm-control unicast** global configuration commands to set up the storm control threshold value.

Storm Control Configuration

This section describes how to configure storm control on your router. It consists of the following configuration information and procedures:

- Enabling Storm Control
- Verifying Storm Control

By default, unicast, broadcast, and multicast suppression is disabled on the switch.

Enabling Storm Control

Enable **storm-control** globally and enter the percentage of total available bandwidth that you want to be used by a all traffic (multicast, unitcast,); entering 100 percent would allow all traffic.

To enable a particular type of storm-control, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] storm-control broadcast threshold <0-100>`	Specifies the broadcast suppression level for an interface as a percentage of total bandwidth. A threshold value of 100 percent means that no limit is placed on broadcast traffic. Use the **no** keyword to restore the defaults.
Step 3	`Router(config)# [no] storm-control multicast threshold <0-100>`	Specifies the multicast suppression level for an interface as a percentage of total bandwidth. Use the **no** keyword to restore the defaults.
Step 4	`Router(config)# [no] storm-control unicast threshold <0-100>`	Specifies the unicast suppression level for an interface as a percentage of total bandwidth. Use the **no** keyword to restore the defaults.
Step 5	`Router(config)# end`	Returns to privileged EXEC mode.

Verifying Storm Control

Use the **show storm-control** command to view switch port characteristics, including the storm control levels set on the interface.

To verify storm-control statistics on an interface, use the following commands, beginning in privileged EXEC mode:

Command	Purpose
show interface [*interface-id*] **counters broadcast**	Verifies the broadcast suppression discard counter for all interfaces or a specific interface. Verify the number of packets discarded.
show interface [*interface-id*] **counters multicast**	Verifies the multicast suppression discard counter for all interfaces or a specific interface. Verify the number of packets discarded.
show interface [*interface-id*] **counters unicast**	Verifies the unicast suppression discard counter for all interfaces or a specific interface. Verify the number of packets discarded.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch "hears" an IGMP report from a host for a given multicast group, the switch adds the host's port number to the Group Destination Address (GDA) list for that group. And, when the switch hears an IGMP leave, it removes the host's port from the content-addressable memory (CAM) table entry.

The purpose of IGMP snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain, and this can consume a lot of bandwidth if many multicast servers are sending streams to the segment.

Multicast traffic is flooded because a switch usually learns MAC addresses by looking into the source address field of all the frames it receives. But, since a multicast MAC address is never used as source address for a packet and since the addresses do not appear in the MAC address table, the switch has no method for learning the addresses.

IGMP Snooping Configuration

IGMP snooping is enabled by default on a VLAN. Multicast routing has to be enabled on the router first and then PIM (Multicast routing protocol) has to be enabled on the VLAN interface so that the switch acknowledges the IGMP join and leave messages which are sent from the hosts connected to the switch. For example:

```
Router(config)# ip multicast-routing
Router(config-if)# interface VLAN1
    ip-address 192.168.10.1 255.255.255.0
    ip pim sparse-mode
```

To verify multicasting support, use the **show ip igmp group** command:

```
Router# show ip igmp group
```

To verify IGMP snooping, use the **show mac-address-table multicast igmp-snooping** command:

```
Router# show mac-address-table multicast igmp-snooping
```

To verify the multicast routing table, use the **show ip mroute** command:

```
Router# sh ip mroute
```

IEEE 802.1Q Configuration

This chapter describes:

- IP Routing over IEEE 802.1Q
- InterVLAN Routing and 802.1Q Trunking

IP Routing over IEEE 802.1Q

This section provides procedures for configuring protocols supported with IEEE 802.1Q encapsulation. The basic process is the same, regardless of the protocol. The process involves the following:

- Enabling the protocol on the router
- Enabling the protocol on the interface
- Defining the encapsulation format as IEEE 802.1Q
- Customizing the protocol to meet the requirements for your environment

To route IP over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform these tasks in the order in which they appear:

- Enabling IP Routing
- Defining the VLAN Encapsulation Format
- Assigning an IP Address to a Network Interface

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers and to define VLAN topologies.

Note IEEE 802.1Q support is available for the MARC 10/100 Fast Ethernet interface only. The FESMIC 10/100 Fast Ethernet interfaces do not support IEEE 802.1Q.

For complete descriptions of the VLAN commands used in this section, refer to the "Cisco IOS Switching Commands" chapter in the *Cisco IOS Switching Services Command Reference*. For descriptions of other commands that appear in this section, you can either use the command reference master index or search online.

Enabling IP Routing

IP routing is automatically enabled in Cisco routers. To reenable IP routing if it has been disabled, use the following command in global configuration mode:

```
Router(config)#ip routing
```

Once you have IP routing enabled on the router, you can customize the characteristics to suit your environment. If necessary, refer to the IP configuration chapters in the *Cisco IOS IP and IP Routing Configuration Guide* for guidelines on configuring IP.

Defining the VLAN Encapsulation Format

To define the encapsulation format as IEEE 802.1Q, use the following commands in interface configuration mode.

	Command	Task
Step 1	**interface FastEthernet** *slot/port.subinterface-number* [1]	Specify the subinterface on which IEEE 802.1Q will be used.
Step 2	**encapsulation dot1q** *vlanid*	Define the encapsulation format as IEEE 802.1Q and specifies the VLAN identifier.

1. If the router supports only port numbers, and not slot numbers, the format for this command is **interface fastethernet** *port.subinterface-number*

Assigning an IP Address to a Network Interface

An interface can have one primary IP address. To assign a primary IP address and a network mask to a network interface, use the following command in interface configuration mode.

Command	Task
ip address *ip-address mask*	Set a primary IP address for an interface.

A mask identifies the bits that denote the network number in an IP address. When you use a mask to subnet a network, that mask is referred to as a *subnet mask*.

Example of IP Routing over IEEE 802.1Q

This configuration example shows IP being routed on VLAN 101:

```
!
ip routing
!
interface fastethernet 0/0.101
  encapsulation dot1q 101
  ip addr 10.0.0.11 255.0.0.0
!
```

VLAN Commands

This section provides an alphabetical listing of useful VLAN commands. All CLI commands used with this feature are documented in the Cisco IOS Release 12.1T (or higher) command reference documents.

Command	Description
`clear vlan statistics`	Removes virtual LAN statistics from any statically configured or system-configured entries.
`debug vlan packets`	Displays general information on virtual LAN (VLAN) packets that the router has received but that it is not configured to support.
`encapsulation dot1q`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs in subinterface configuration mode.
`show vlans`	Displays VLAN subinterfaces.

InterVLAN Routing and 802.1Q Trunking

This document provides sample 802.1Q trunking configurations between a Catalyst 3512-XL switch and a Cisco 2600 router; the results of each command are displayed as they are executed. Cisco routers with FastEthernet interfaces, and any Catalyst 2900XL, 3500XL, or 2950 switch can be used in the scenarios presented in this document to obtain the same results.

Trunking is a way to carry traffic from several VLANs over a point-to-point link between the two devices. Ethernet trunking can be implemented by using 802.1Q.

We will create a trunk that carries traffic from two VLANs (VLAN1 and VLAN2) across a single link between a Catalyst 3500 and a Cisco 2600 router. We are using the Cisco 2600 router to do the Inter-VLAN routing between VLAN1 and VLAN2.

Layer 2 switches are not capable of routing or communicating between the VLANs.Therefore, the 10/100 Fast Ethernet interface on the router (FastEthernet 0/0) will support a VLAN, but the 10/100 Fast Ethernet interface on the FESMIC switch (FastEthernet 0/0) will not support a VLAN. For further details on Inter-VLAN routing, refer to the Routing Between Virtual LANs Overview chapter of the "Cisco IOS Switching Services Configuration Guide," release 12.1.

Router Description

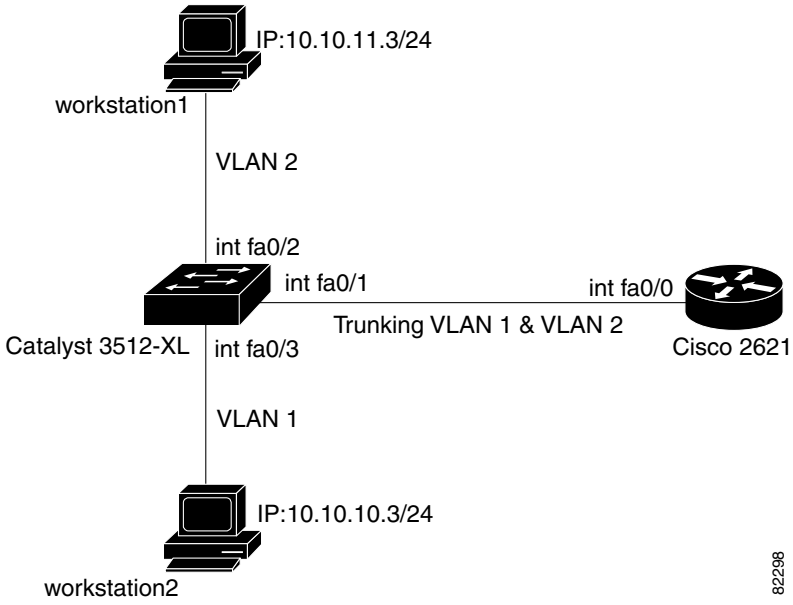
For 802.1Q trunking, one VLAN is not tagged. This VLAN is called native VLAN. The native VLAN is used for untagged traffic when the port is in 802.1Q trunking mode. While configuring 802.1Q trunking, keep in mind that the native VLAN must be configured the same on each side of the trunk link. It is a common mistake not to match the native VLANs while configuring 802.1Q trunking between the router and the switch. For details on native VLANs, refer to the IEEE 802.1Q section, of "Bridging Between IEEE 802.1Q VLANs," in New Features in release 12.1(3)T.

In this sample configuration, the native VLAN is VLAN1 by default on both the Cisco 2621 router and the Catalyst 3512XL switch. Depending on your network needs, you might have to use a native VLAN other than the default, VLAN1. Commands in the configurations section of this document describe how to change the native VLAN on the Cisco 2600 router and Catalyst 3500XL switch.

Sample configurations presented in this document can be used on the Cisco 3200 Series router, as it includes at least one 10/100 Fast Ethernet interface. Also, make sure that you are using the Cisco IOS version that supports ISL/802.1Q VLAN trunking.

For more information, see the Cisco Technical Tips Conventions.

Figure 15-1 Network Diagram



Switch Configuration

The following example show the commands that were entered on the 3512XL switch:

Step 1 Set the privileged mode and Telnet password on the switch.

```
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#hostname 3512xl
3512xl(config)#enable password mysecret
3512xl(config)#line vty 0 4
3512xl(config-line)#login
3512xl(config-line)#password mysecret
3512xl(config-line)#exit
3512xl(config)#no logging console
3512xl(config)#^Z
```

Step 2 Set the IP address and default gateway for VLAN1 for management purposes.

```
3512xl#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3512xl(config)#int vlan 1
3512xl(config-if)#ip address 10.10.10.2 255.255.255.0
3512xl(config-if)#exit
3512xl(config)#ip default-gateway 10.10.10.1
3512xl(config)#end
```

Step 3 Set the `device to` VTP `TRANSPARENT` mode.

In our example, we set the mode to be transparent. Depending on your network, set the VTP Mode accordingly. For details on VTP, refer to "Configuring VTP, VLANs, and VLAN Trunks on Catalyst 2900XL and 3500XL Switches."

```
3512xl#vlan database
3512xl(vlan)#vtp transparent
Setting device to VTP TRANSPARENT mode.
```

Step 4 Add VLAN2. (VLAN1 already exists by default.)

```
512xl(vlan)#vlan 2
VLAN 2 added:
Name: VLAN0002
3512xl(vlan)#exit
APPLY completed.
Exiting....
```

Step 5 Enable trunking on the interface FastEthernet 0/1.

```
3512xl#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
512xl(config)#int FastEthernet 0/1
512xl(config-if)#switchport mode trunk
```

Step 6 Enter the trunking encapsulation as either isl,

```
512xl(config-if)#switchport trunk encapsulation isl
```

or as **dot1q**

```
512xl(config-if)#switchport trunk encapsulation dot1q
```

In case of Cisco 2950 switches, the above two commands are not used. Cisco 2950 switches only support 802.1Q encapsulation, which is configured automatically, when trunking is enabled on the interface by using switchport mode trunk command.

In case of dot1q, make sure that the native VLAN matches across the link. On 3512XL, by default, the native VLAN is 1. Depending on your network needs, you can change the native VLAN to be other than VLAN1, but it is important that you change the native VLAN on the router accordingly. You can change the native VLAN, if needed, by using the following command:

```
3512xl(config-if)#switchport trunk native vlan <vlanID>
```

Step 7 Allow all VLANs on the trunk.

```
3512xl(config-if)#switchport trunk allowed vlan all
3512xl(config-if)#exit
```

Step 8 Place FastEthernet 0/2 into VLAN2 and enable portfast on the interface.

```
3512xl(config)#int FastEthernet 0/2
3512xl(config-if)#switchport access vlan 2
3512xl(config-if)#spanning-tree portfast
3512xl(config-if)#exit
```

Step 9 FastEthernet 0/3 is already in VLAN1 by default. Enable portfast on the interface.

```
3512xl(config)#int FastEthernet 0/3
3512xl(config-if)#spanning-tree portfast
3512xl(config-if)#^Z
```

For details on why you should enable portfast, refer to "Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays."

Step 10 Save the configuration.

```
3512xl#write memory
Building configuration...

3512xl#
```

Step 11 Verify the configuration as follows:

```
3512xl#show running-config
 Building configuration...

 Current configuration:

!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3512xl
!
no logging console
enable password mysecret
 !
ip subnet-zero
!
interface FastEthernet0/1
switchport mode trunk
```

If 802.1Q is configured, you will instead see the following output under interface FastEthernet 0/1:

```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 2
  spanning-tree portfast
!
interface FastEthernet0/3
  spanning-tree portfast
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface VLAN1
  ip address 10.10.10.2 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
!
ip default-gateway 10.10.10.1
!
line con 0
  transport input none
  stopbits 1
```

```
line vty 0 4
 password mysecret
 login
line vty 5 15
 login
!
end
```

Router Configuration

The following examples show the commands that were entered on the Cisco 2600 router.

Step 1 Set the privileged mode and Telnet password on the router.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname c2600

c2600(config)#enable password mysecret
c2600(config)#line vty 0 4
c2600(config-line)#login
c2600(config-line)#password mysecret
c2600(config-line)#exit
c2600(config)#no logging console
c2600(config)#^Z

c2600#configure terminal
```

Step 2 Select FastEthernet 0/0 for the trunk configuration. No L2 or Layer 3 (L3) configuration is done here.

```
c2600(config)#int FastEthernet 0/0
c2600(config-if)#no shut
c2600(config-if)#exit
```

Step 3 Enable trunking on the sub-interface FastEthernet 0/0.1. Note that actual trunks are configured on the sub-interfaces.

```
c2600(config)#int FastEthernet 0/0.1
```

Step 4 Enter the trunking encapsulation as either **isl**

```
c2600(config-subif)#encapsulation isl 1
```

or as **dot1q**. In case of dot1q, you need to make sure that the native VLAN matches across the link. On 3512XL, by default, the native VLAN is 1. On the router, configure VLAN1 as the native VLAN.

```
c2600(config-subif)#encapsulation dot1Q 1 native
```

On the switch, if you have a native VLAN other than VLAN1, on the router, configure the same VLAN to be the native VLAN, by using the above command.

The following example configures 802.1Q trunking on the router.

Step 1 Configure L3 information on the sub-interface 0/0.1.

```
c2600(config-subif)#ip address 10.10.10.1 255.255.255.0
c2600(config-subif)#exit
```

Step 2 Enable trunking on the sub-interface FastEthernet 0/0.2. Note that actual trunks are configured on the sub-interfaces.

```
c2600(config)#int FastEthernet 0/0.2
```

Step 3 Enter the trunking encapsulation as either **isl**

```
c2600(config-subif)#encapsulation isl 2
```

or as **dot1q**:

```
c2600(config-subif)#encapsulation dot1Q 2
```

Step 4 Configure L3 information on the sub-interface 0/0.2.

```
c2600(config-subif)#ip address 10.10.11.1 255.255.255.0
c2600(config-subif)#exit
c2600(config)#^Z
```

Step 5 Save the configuration:

```
c2600#write memory
Building configuration...
[OK]
c2600#
```

To make this setup work, and to successfully ping between workstation1 and workstation2, make sure that the default gateways on the workstations are setup properly. For workstation1, the default gateway should be 10.10.11.1 and for workstation2, the default gateway should be 10.10.10.1. For details on how to set the default gateways on the workstations, refer to their respective sections in this document.

802.1Q Configuration on the Router for Cisco IOS Versions Earlier than 12.1(3)T

As described earlier in this document, while configuring 802.1Q trunking it is very important to match the native VLAN across the link. In the Cisco IOS software versions earlier than 12.1(3)T, you cannot define the native VLAN explicitly, as the encapsulation dot1Q 1 native command under the sub-interface is not available.

In the earlier Cisco IOS versions, it is important not to configure VLAN1 interface as a sub-interface. The router then expects a tag dot1q frame on VLAN1 and the switch is not expecting a tag on VLAN1. As a result, no traffic will pass between VLAN1 on the switch and the router.

Use the following steps to configure the Cisco 2600 router:

Step 1 Set the privileged mode and Telnet password on the router.

```
Router#configure terminal
Router(config)#hostname c2600
c2600(config)#enable password mysecret
c2600(config)#line vty 0 4
c2600(config-line)#login;
c2600(config-line)#password mysecret
c2600(config-line)#exit
c2600(config)#no logging console
```

Step 2 Select FastEthernet 0/0 for the trunk configuration.

```
c2600(config)#int FastEthernet 0/0
c2600(config-if)#no shut
```

Note that the IP address for VLAN1 is configured on the main interface, and no encapsulation for VLAN1 will be done under the sub-interface.

```
c2600(config-if)#ip address 10.10.10.1 255.255.255.0
c2600(config-if)#exit
```

Step 3 Configure dot1q encapsulation for VLAN 2 on sub-interface fastEthernet 0/0.2.

```
c2600(config)#int FastEthernet 0/0.2
c2600(config-subif)#encapsulation dot1Q 2
```

Step 4 Configuring L3 information on the sub-interface 0/0.2.

```
c2600(config-subif)#ip address 10.10.11.1 255.255.255.0
c2600(config-subif)#exit
c2600(config)#^Z
```

Step 5 Save the configuration.

```
c2600#write memory
Building configuration...
[OK]
c2600#
```

To successfully ping between workstation1 and workstation2, you need to make sure that the default gateways on the workstations are setup properly. For workstation1, the default gateway should be 10.10.11.1, and for workstation2, the default gateway should be 10.10.10.1. For details on how to set the default gateways on the workstations, refer to thei respective sections in this document.

debug and show Commands

Use the **show int** {**FastEthernet**} command to check the administrative and operational status of the port. It is also used to make sure that the native VLAN matches on both sides of the trunk. The native VLAN is used for untagged traffic when the port is in 802.1Q trunking mode.

```
3512xl#show int FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: isl
```

```
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

For 802.1Q trunking, the output of the above command changes as follows:

```
Router#show int FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
```

show vlans Command

Use the **show vlans** command on the MARC to verify that the 10/100 Fast Ethernet interface (port) belongs to the correct VLAN. In our example, only interface FastEthernet 0/0 belongs to VLAN2. The rest are members of VLAN1.

```
3512xl#show vlans
VLAN Name                      Status   Ports
---- ------------------------- -------- --------------------------------
1    default                   active   Fa0/3, Fa0/4
2    VLAN0002                  active    Fa0/0
1002 fddi-default              active
1003 token-ring-default            active
1004 fddinet-default               active
1005 trnet-default                 active

...(output suppressed)
```

show vlan-switch Command

Use the **show vlan-switch** command on the FESMIC interfaces to verify that the interface (port) belongs to the correct VLAN.

```
virgoa1#sh vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------
1    default                          active
2    VLAN0002                         active    Fa3/0, Fa3/1
3    VLAN0003                         active
```

```
4    VLAN0004                         active
5    VLAN0005                         active    Fa3/3
6    VLAN0006                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1003  tr      101003      1500   1005   0      -        -    srb      1      1002
1004 fdnet 101004    1500  -      -      1        ibm  -        0      0
1005 trnet 101005    1500  -      -      1        ibm  -        0      0
```

show vtp status Command

This command is used to check the VLAN trunking protocol (VTP) configuration on the switch. In our example, we have used transparent mode. The correct VTP mode depends on the topology of your network. For details on VTP, refer to Configuring VTP, VLANs, and VLAN Trunks on Catalyst 2900XL and 3500XL Switches.

```
3512xl#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally  : 254
Number of existing VLANs        : 6
VTP Operating Mode              : Transparent
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xC3 0x71 0xF9 0x77 0x2B 0xAC 0x5C 0x97
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

show vlan Command

This command tells you what L2 or L3 information is configured for each VLAN.

```
c2600#show vlan

Virtual LAN ID:  1 (Inter Switch Link Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.1

   Protocols Configured:   Address:              Received:        Transmitted:
     IP              10.10.10.1        40             38

Virtual LAN ID:  2 (Inter Switch Link Encapsulation)
```

```
   vLAN Trunk Interface:   FastEthernet0/0.2

   Protocols Configured:   Address:              Received:        Transmitted:
     IP              10.10.11.1        9              9
```

For 802.1Q trunking, the output of the above command changes as follows:

```
c2600#show vlan

Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.1
```

This is configured as native Vlan for the following interface(s): FastEthernet0/0

```
   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.10.10.1                 0                  2

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.2

   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.10.11.1                42                 19
```

For 802.1Q trunking, with Cisco IOS versions earlier then 12.1(3)T, the output of the command changes as follows:

```
c2600#show vlan

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.2

   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.10.11.1                 6                  4
```

No IEEE 802.1Q encapsulation is displayed for VLAN1 on any of the sub-interfaces.

show interface Command

Use the **show interfaces** command to check the administrative and operational status of the interface.

```
c2600#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     217 packets input, 12884 bytes
     Received 217 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     45 packets output, 6211 bytes, 0 underruns(0/0/0)
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

c2600#show interfaces FastEthernet 0/0.1
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ISL Virtual LAN, Color 1.
  ARP type: ARPA, ARP Timeout 04:00:00

c2600#show interfaces FastEthernet 0/0.2
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
  Internet address is 10.10.11.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ISL Virtual LAN, Color 2.
  ARP type: ARPA, ARP Timeout 04:00:00
```

For 802.1Q trunking, the output of the above command changes as follows:

```
c2600#show interfaces FastEthernet 0/0.1
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1.
  ARP type: ARPA, ARP Timeout 04:00:00

c2600#show interfaces FastEthernet 0/0.2
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
  Internet address is 10.10.11.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  2.
  ARP type: ARPA, ARP Timeout 04:00:00
```

CHAPTER 16

MIB Support

This chapter describes the MIBs supported by Cisco 3200 Series Mobile Access Routers.

General MIBs

- BRIDGE-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CIRCUIT-INTERFACE-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NTP-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-PROCESS-MIB
- CISCO-STACKMAKER-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB

- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- RFC 1213-MIB (MIBII)
- SNMPv2-MIB

Wireless MIBs

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOLFILTER-MIB
- CISCO-SYSLOG-EVENTEXT-MIB
- CISCO-TBRIDGE-DEV-IFMIB

Routing and Routed Protocol MIBs

- CISCO-MOBILE-IP-MIB
- CISCO-PING-MIB
- CISCO-TCP-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-TCP-MIB
- RFC 1253-MIB (OSPF)
- TCP-MIB
- UDP-MIB
- RFC 2006-MIB
- BGP4-MIB
- CISCO-BGP4-MIB

LAN and WAN MIBs

- RFC 1398-MIB (Ethernet)
- CISCO-DIAL-CONTROL-MIB
- CISCO-FRAME-RELAY-MIB
- RFC 1315-MIB (Frame Relay)
- RFC 1381-MIB (LAPB)
- RFC1382-MIB (X.25)
- RS-232-MIB

IP Multicasting MIBs

- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- IGMP-STD-MIB
- IPMROUTE-MIB
- IPMROUTE-STD-MIB
- MSDP-MIB
- PIM-MIB

IPSEC/VPN MIBs

- CISCO-IPSEC-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-POLICY-MAP-MIB
- CISCO-VPDN-MGMT-MIB

QOS MIBs

- CISCO-CAR-MIB
- CISCO-IP-STAT-MIB
- CISCO-QUEUE-MIB
- INT-SERV-MIB
- INT-SERV-GUARANTEED-MIB
- RSVP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-PPPOE-MIB

Network Management MIB

- CISCO-RTTMON-MIB

VLAN MIBs

- CISCO- VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

Mobile IP MIB Support

The Mobile IP MIB support for the Simple Network Management Protocol (SNMP) feature adds a MIB module that expands network monitoring and management capabilities of foreign agent and home agent Mobile IP entities. Mobile IP management using SNMP is defined in two MIBs: the RFC 2006-MIB and the CISCO-MOBILE-IP-MIB.

The RFC 2006-MIB is a MIB module that uses the definitions defined in RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*. Beginning in Cisco IOS Release 12.2(1)T, RFC 2006 set operations and an SNMP notification (trap) are supported. Set operations, performed from a network management system (NMS), allow you to use the RFC 2006-MIB objects for starting and stopping the Mobile IP service, modifying and deleting security associations, modifying advertisement parameters, and configuring care-of addresses for foreign agents. An SNMP notification for security violations can also be enabled on supported routing devices using the IOS software.

The CISCO-MOBILE-IP-MIB is a Cisco enterprise-specific extension to the RFC 2006-MIB. The CISCO-MOBILE-IP-MIB allows you to monitor the total number of home agent mobility bindings and the total number of foreign agent visitor bindings using an NMS. These bindings are defined in the CISCO-MOBILE-IP-MIB as *cmiHaRegTotalMobilityBindings* and *cmiFaRegTotalVisitors*, respectively.

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

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

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

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

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

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

http://www.cisco.com/register

Mobile IP MIB Benefits

The RFC 2006-MIB defines a notification for Mobile IP entities (home agent or foreign agent) that can be sent to an NMS if there is a security violation. This notification can be used to identify the source of intrusions.

The RFC 2006-MIB also defines a table (*mipSecViolationTable*) to log the security violations in the Mobile IP entities. This log can be retrieved from an NMS (using Get operations) and can be used to analyze the security violation instances in the system.

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

Mobile IP MIB Restrictions

The following restrictions exist for using Set operations on the following objects and tables in the RFC 2006 MIB:

- mipEnable object—This object can be used to start and stop the Mobile IP service on the router. There are no issues with the Set support for this object.
- faRegistrationRequired object—This object controls whether the mobile node should register with the foreign agent. The Cisco implementation of Mobile IP allows configuring this parameter at an interface level through the command line interface. However, this object is not defined at the interface level in the MIB. Therefore, no SNMP operation is permitted on this object.
- mipSecAssocTable—This table allows the Management Station to view/modify the existing the configuration of security association between different Mobile IP entities (home agent, foreign agent, and mobile node). The index objects for this table are the IP address of the entity and the security parameter index (SPI). No object is provided for creation or deletion of new rows in this table via SNMP. Table 16-1 shows the fixed values for objects in the mipSecAssocTable.

Table 16-1 Fixed Security Method for RFC 2006-MIB mipSecAssocTable Objects

Object	Fixed Security Method Value
mipSecAlgorithmType	MD5
mipSecAlgorithmMod	prefixSuffix
mipSecReplayMethod	timestamps

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

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

- maAdvConfigTable—This table allows modification of advertisement parameters of all advertisement interfaces in the mobility agent. Even though this table has a rowStatus object, row creation and destroy is not possible because creating a new row implies that a home agent or foreign agent service should be started on the interface corresponding to the new row.

  But no object in this table specifies the service (home agent or foreign agent) to be started. Therefore, there should already be one row corresponding to each interface on which the foreign agent or home agent service is enabled.

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

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

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

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

Send Mobile IP MIB Notifications

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

To configure the router to send Mobile IP traps or informs to a host, use the following commands in global configuration mode.

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

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

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

Mobile IP Security Violation Notification Configuration Example

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

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

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the **no** form of this command.

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must identify at least one **snmp-server host**.

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

Note If the *community-string* is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, although an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** global configuration command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** global configuration command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** global configuration command. These notification types do not require an **snmp-server enable** command.

Availability of a notification-type option depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To learn which notification types are available on your system, use the **?** command at the end of the **snmp-server host** command.

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access list. In the following example, the community string is named comaccess and the access list is numbered 10:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

The following example sends RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server enable traps snmp
snmp-server enable traps envmon
snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com informs version 2c public hsrp
```

Workgroup Bridge SNMP Link Traps Example

For a workgroup bridge to generate the SNMP link trap, the following SNMP commands should be entered on the bridge.

```
snmp-server trap-source Dot11Radio0
snmp-server enable traps snmp linkdown linkup
snmp-server host 1.7.35.35 version
```

The IP address of the device receiving the trap should be the static IP address of the loopback interface on the mobile access router instead of the IP address of the Fast Ethernet VLAN interface, because the Fast Ethernet interfaces IP addresses will be dynamic when dynamic host configuration protocol (DHCP) is enabled.

To force the SNMP packets that are typically sent to the Fast Ethernet interface on the mobile access router to be sent to the loopback interface, the following command should also be entered.

arp *1.7.35.35 00ff.ff40.0087* **ARPA BVI1**

where *1.7.35.35 00ff.ff40.0087* is the MAC address of the Fast Ethernet interface on the mobile access router.

To forward the SNMP packet and the non-native VLAN traffic generated by the workgroup bridge associated with a root device in a VLAN environment in infrastructure mode, VLAN trunking should be turned on for the mobile access router Fast Ethernet interface. The **wgb vlan** command should not be configured on the WGB.

You must add a loopback interface with an IP address on workgroup bridge because the SNMP manager on mobile access router needs a static IP address on workgroup bridge side. The following is an example of SNMv3 configuration.

Workgroup Bridge

```
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 noauth
snmp-server user labusr labgrp v3
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 noauth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3
snmp-server group labgrp v3 noauth
snmp-server manager
snmp-server manager session-timeout <num>
2.authNoPriv:
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 auth
snmp-server user labusr labgrp v3 auth md5 MD5passwd
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 auth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3 auth md5 MD5passwd
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout <num>
```

FTP the MIB Files

Follow these steps to obtain each MIB file by using FTP:

Step 1 Use FTP to access the server **ftp.cisco.com**.

Step 2 Log in with the username **anonymous**.

Step 3 Enter your e-mail username when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to **/pub/mibs/v1** or **/pub/mibs/v2**.

Step 5 Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

Note You can also access information about MIBs on the Cisco web site: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on your mobile node.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference* for this release and to the *Cisco IOS Configuration Fundamentals Command Reference* for this release.

This chapter consists of these sections:

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and management information base (MIB) reside on the network device. To configure SNMP, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1 is a full Internet standard, defined in RFC 1157.
- SNMPv2C, which has these features:

  - SNMPv2, a draft Internet standard, defined in RFCs 1902 through 1907.
  - SNMPv2C, an experimental Internet protocol defined in RFC 1901.
- SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network, defined in RFC 2273, RFC 2274, and RFC 2275.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the Community-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; therefore, you can configure the software to support communications with one management station using the SNMPv1 protocol and another using the SNMPv2 protocol.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 17-1.

Table 17-1 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]
get-bulk-request[2]	Retrieves large blocks of data that would otherwise require the transmission of many small blocks of data, such as multiple rows in a table.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command works only with SNMPv2.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the bridge, the community string definitions on the NMS must match at least one of the three community string definitions on the bridge.

A community string can have one of these attributes:

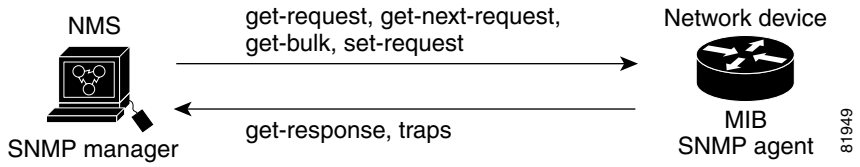
- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 software uses the bridge MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetwork problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 17-1, the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 17-1 SNMP Network



For information on supported MIBs and how to access them, see Chapter 16, “MIB Support”

Configuring SNMP

This section describes how to configure SNMP on your bridge.

Default SNMP Configuration

Table 17-2 shows the default SNMP configuration.

Table 17-2 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	None configured
SNMP trap receiver	None configured
SNMP traps	None enabled

Enabling the SNMP Agent

No specific IOS command exists to enable SNMP. The first **snmp-server** global configuration command that you enter enables SNMPv1 and SNMPv2.

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the bridge.

Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Note In the current IOS MIB agent implementation, the default community string is for the Internet MIB object sub-tree. Because IEEE802dot11 is under another branch of the MIB object tree, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree. ISO is the common parent node of IEEE (IEEE802dot11) and Internet. This MIB agent behavior is different from the MIB agent behavior on access points not running IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the bridge:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	Configure the community string. • For *string*, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. • (Optional) For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. • (Optional) For **view** *mib-view*, specify a MIB view to which this community has access, such as **ieee802dot11**. See the "Using the snmp-server view Command" section on page 17-8 for instructions on using the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view. • (Optional) Specify either read-only (**ro**) if you want authorized management stations to retrieve MIB objects, or specify read/write (**rw**) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. **Note** To access the IEEE802dot11 MIB, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 2. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string). To remove a specific community string, use the **no snmp-server community** *string* global configuration command.

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the device generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Devices can have an unlimited number of trap managers. Community strings can be any length.

Table 17-3 describes the supported bridge traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 17-3 Notification Types

Notification Type	Description
authenticate-fail	Enable traps for authentication failures.
config	Enable traps for SNMP configuration changes.
deauthenticate	Enable traps for client device deauthentications.
disassociate	Enable traps for client device disassociations.
dot11-qos	Enable traps for QoS changes.
entity	Enable traps for SNMP entity changes.
envmon temperature	Enable traps for monitoring radio temperature. This trap is sent out when the bridge radio temperature approaches the limits of its operating range (55 C to -33 C; 131 F to -27.4 F).
linkDown	The interface keeps any DHCP-acquired IP address. Receipt of a valid linkDown trap starts a new link-down hold-down timer.
linkUp	When a linkUp trap event occurs, the DHCP client must either renew the current IP address or acquire a new IP address as quickly as possible.
snmp	Enable traps for SNMP events.
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.

Some notification types cannot be controlled with the **snmp-server enable** global configuration command, such as **tty** and **udp-port**. These notification types are always enabled. You can use the **snmp-server host** global configuration command to a specific host to receive the notification types listed in Table 17-3.

Beginning in privileged EXEC mode, follow these steps to configure the bridge to send traps to a host:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	Specify the recipient of the trap message. • For *host-addr,* specify the name or address of the host (the targeted recipient). • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify the string to send with the notification operation. Though you can set this string using the **snmp-server host** command, Cisco recommends that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the keywords listed in Table 17-3 on page 17-6.
Step 3	**snmp-server enable traps** *notification-types*	Enable the bridge to send specific traps. For a list of traps, see Table 17-3 on page 17-6. To enable multiple types of traps, you must issue a separate **snmp-server enable traps** command for each trap type.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server contact** *text*	Set the system contact string. For example: `snmp-server contact Dial System Operator at beeper 21555.`
Step 3	**snmp-server location** *text*	Set the system location string. For example: `snmp-server location Building 3/Room 222`
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Using the snmp-server view Command

In global configuration mode, use the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view and the dot11 read-write community string.

This example shows how to enable IEEE view and dot11 read-write community string:

```
bridge(config)# snmp-server view ieee ieee802dot11 included
bridge(config)# snmp-server community dot11 view ieee RW
```

SNMP Examples

This example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the bridge to send any traps.

```
bridge(config)# snmp-server community public
```

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The bridge also sends configuration traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
bridge(config)# snmp-server community public
bridge(config)# snmp-server enable traps config
bridge(config)# snmp-server host 192.180.1.27 version 2c public
bridge(config)# snmp-server host 192.180.1.111 version 1 public
bridge(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
bridge(config)# snmp-server community comaccess ro 4
bridge(config)# snmp-server enable traps snmp authentication
bridge(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the bridge to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host *cisco.com*.

```
bridge(config)# snmp-server enable traps entity
bridge(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the bridge to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
bridge(config)# snmp-server enable traps
bridge(config)# snmp-server host myhost.cisco.com public
```

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

The following is sample output from the **show snmp** command:

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
    0 Bad SNMP version errors
    4 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs
78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
```

```
    0 General errors
    24 Response PDUs
    13 Trap PDUs

SNMP logging: enabled

    Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
Informs in flight 0/25 (current/max)
Logging to 171.69.217.141.162
4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
Logging to 171.69.58.33.162
0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Troubleshooting the Cisco 3200 Series Mobile Access Router

This document provides some information on troubleshooting a Cisco 3200 Series router. It includes the following:

- Wireless Card Default Configuration Recovery
- Disaster Recovery with TFTP Download
- Access ROM Monitor Mode
- Cisco IOS Image Download from the Console Port
- WMIC Image Update over FESMIC Port
- Flash and NVRAM File Management
- Mobile IP Debug
- Configuration Register Modification
- Password Recovery

Here are some important points to remember in troubleshooting Mobile IP clients:

- Mobile IP clients transmit type 10 ICMP Router Discovery Protocol packets to trigger the Mobile IP process. Routers respond with type 9 ICMP router advertisement packets. After this initial phase, the registration or deregistration process occurs.
- The hold time in the IRDP messages determines how fast the mobile node can detect movement between subnets. For example, the lifetime in the command **ip mobile host 10.0.150.200 interface FastEthernet0/0 lifetime 180** only makes the mobile node reregister with the home agent by using the current agent. It does not force it to switch agents (interfaces).
- The default hold time for IRDP is 30 minutes.

When the home agents or foreign agents advertise, they put a time limit (hold time) in the IRDP advertisements that tells the mobile node the interval the advertisements are valid. When a mobile node moves to a different subnet, the router waits until the hold time expires before it associates with a new interface (agent). If the lifetime on the registration expires before the hold time expires, the mobile node transmits a solicitation for the old agent (interface), until the hold time in the previous agent advertisement expires. If you do not adjust the IRDP timers, for 30 minutes the mobile node does not know that it has changed subnets.

Listed below are basic troubleshooting tips.

- Adjust the interval value for the foreign agent using the **ip irdp maxadvertinterval** *seconds* interface configuration command. Begin by setting the timer to 10 seconds and adjust as needed.
- Before you can ping a subnet on the mobile device, you must first define the subnet on the home agent.
- Redistribute mobile subnets on the home agent so that return traffic can be sent back to the mobile access router.
- Establish a return route from the foreign agent to the home agent.
- Avoid placing any routers behind the mobile device because it functions as a stub router.
- Ensure that the MD5 keys match between the mobile device and the home agent. Authentication is required.

Caveats and Error Messages

The following caveats and error messages apply to the Cisco 3200 Series Mobile Access Router.

Non-Cisco Components

Cisco does not provide:

- Power supply
- Cable assemblies
- Enclosure
- Stacking hardware
- Extractor tools
- Thermal solutions

Non-Cisco Cards

We recommend that you do not add non-Cisco cards that produce peripheral component interconnect (PCI) bus signals. Adding non-Cisco cards that generate PCI bus signals can produce unpredictable results. (Cisco cards do not use ISA bus signals, but all the cards will pass the ISA signals through the bus.)

Cisco MIC Mismatch Error

Most of the Mobile Access Router Card (MARC) stacks are fixed configuration and the stack cannot be modified. The router generates the following error message if the cards are stacked in the router improperly or a MIC in the stack is not supported by the companion MARC.

The following error message is displayed:

```
**************************************************************************
 *            ****NON RECOVERABLE ERROR OCCURRED ****                     *
 *                                                                        *
 *   1) The three cards (3220MARC, 3220SMIC and 3220FESMIC) must be       *
 *      plugged in for the 3220 Mobile Router to be operational.          *
 *                                                                        *
 *   2) The following cards are unsupported                               *
 *      card in slot 1 is 3201SMIC                                       *
 *      card in slot 2 is an unknown card                               *
 *                                                                        *
 *   3) Please power down the router and remove any unsupported cards     *
 *      plugged into the 3220MARC.                                        *
 *                                                                        *
 *   For more information, please refer to the user documentation         *
 *                                                                        *
 **************************************************************************
```

After displaying the error message, the router goes into ROMMON mode. You must modify the card stack before the router will boot by using the Cisco IOS.

Rotary Switch Position Error

The router generates the following error message if the rotary switch is set in a position that is unsupported.

```
**************************************************************************
 *          ****ROTARY SWITCH CONFIGURATION ERROR****                     *
 *                                                                        *
 *   One of the MICs has the rotary switch wrongly configured at          *
 *   position 3. Please change rotary switch configuration on this MIC    *
 *   to a valid position as described below.                              *
 *                                                                        *
 *   Both the MICs with switch positions at 2 and 3 are disabled.         *
 *    Instructions:                                                       *
 *      1) Only switch positions 0-2 are supported.                       *
 *      2) Selecting the same switch position on multiple MICs is not     *
 *         supported.                                                     *
 *      3) To change switch configuration please power down router.       *
 *                                                                        *
 *   For more information, please refer to the hardware documentation.    *
 *                                                                        *
 **************************************************************************
```

After displaying the error message, the router goes into ROMMON mode. You must modify the rotary switch before the router will boot by using the Cisco IOS.

Wireless Card Default Configuration Recovery

It is possible that you might be locked out of the Wireless Mobile Interface Card (WMIC) as the result of an error in an access list or typo in a password. These parameters are stored in the config.txt file in Flash memory.

Caution This procedure erases the wireless card configuration. If you delete the configuration and do not have a copy, you will have to create the configuration from scratch.

To recover control of the router, connect a terminal to the console port of the WMIC and do the following:

Step 1 Enter the **reload** command.

```
c3201br#reload
```

Step 2 Press the Escape (ESC) key twice when the boot process begins to display a bootloader prompt.

```
System configuration has been modified. Save? [yes/no]: yes
Proceed with reload? [confirm]
Radio system: delayed or multiple reload request, ignored
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:02:31.770: %SYS-5-RELOAD: Reload requested by console.Xmodem
file system is available.
flashfs[0]: 136 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 8169984
flashfs[0]: Bytes available: 7828992
flashfs[0]: flashfs fsck took 34 seconds.
Base ethernet MAC Address: 00:05:9a:3d:32:01
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
ethernet link up, 100 mbps, full-duplex
Ethernet port 0 initialized: link is up
Loading
"flash:/c3201-k9w7-mx.122/c3201-k9w7-mx.122"...##########################################
##################################################################bad
mzip file, unknown zip method

Error loading "flash:/c3201-k9w7-mx.122/c3201-k9w7-mx.122"

Interrupt within 5 seconds to abort boot process.
Boot process terminated.

The system is unable to boot automatically. The BOOT
environment variable needs to be set to a bootable
image.

C3201 Boot Loader (C3201-BOOT-M), Version 12.2 [hftseng-c3201wmic 102]
compiled Sun 29-Feb-04 15:59 by hftseng

bridge:
```

Step 3 Enter the **dir flash:** command to verify the config.txt file is in memory.

```
bridge: dir flash:
Directory of flash:/
```

```
2    -rwx  4114432   <date>              c3201-k9w7-tar
3    -rwx  180       <date>              env_vars
4    -rwx  1091      <date>              config.txt
5    drwx  384       <date>              c3201-k9w7-mx.122
142  -rwx  1091      <date>              config.txt.saved
143  -rwx  5         <date>              private-config

7828992 bytes available (8169984 bytes used)
```

Step 4 Enter the **delete flash:config.txt** command.

```
bridge: delete flash:config.txt
Are you sure you want to delete "flash:config.txt" (y/n)?y
File "flash:config.txt" deleted

bridge:
```

Step 5 Reboot the router.

Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the command–line interface (CLI). However, if the router is unable to boot the Cisco IOS software, you can load new software while in ROM monitor mode.

This section describes how to load a Cisco IOS software image from a remote TFTP server to the router Flash memory.

The following steps should be performed while in ROM monitor mode.

Step 1 Use the appropriate commands to enter all the required variables and any optional variables described earlier in this section.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld -r
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to Flash memory. You can then use the image that is in Flash memory the next time you enter the **reload** command.

You will see output similar to the following:

```
rommon 4 > tftpdnld

          IP_ADDRESS: 1.6.88.21
      IP_SUBNET_MASK: 255.255.0.0
     DEFAULT_GATEWAY: 1.6.0.1
         TFTP_SERVER: 223.255.254.251
           TFTP_FILE: cisco/c3200-i11k9-mz.bin
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter y in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router begins to download the new file.

Entering Ctrl-C or Break stops the transfer before the Flash memory is erased.

TFTP Download Command Variables

This section describes the system variables that can be set in ROM monitor mode and that are used during the TFTP download process.

Note The commands described in this section are case-sensitive and must be entered exactly as shown in the tables.

Required Variables

These variables must be set with these commands before using the **tftpdnld** command:

Command	Description
IP_ADDRESS= *ip_address*	IP address of the router.
IP_SUBNET_MASK= *ip_address*	Subnet mask of the router.
DEFAULT_GATEWAY= *ip_address*	IP address of the default gateway of the router.
TFTP_SERVER= *ip_address*	IP address of the TFTP server from which the software will be downloaded.
TFTP_FILE= *filename*	The name of the file that will be downloaded to the router.

Optional Variables

These variables can be set with these commands before using the **tftpdnld** command:

Variable	Command
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process; for example: `Initializing interface.` `Interface link state up.` `ARPing for 1.4.0.1` `ARP reply for 1.4.0.1 received.  MAC address 00:00:0c:07:ac:01`	**TFTP_VERBOSE=** *setting*

Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Amount of time, in seconds, before the download process times out. The default is 2, 400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Access ROM Monitor Mode

The ROM monitor firmware runs when the router is powered up or reset and helps to initialize the processor hardware and boot the operating system software. If there is no Cisco IOS software image loaded on the router, ROM monitor is the default operating system. If there is an Cisco IOS software image, you can still force the router to boot to the ROM monitor by pressing the break key within the first 60 seconds of the router booting or changing the configuration register so the router looks for the ROM monitor bootable image first. In ROM monitor mode, you can perform certain configuration tasks, such as to boot without loading the configuration file to recover a lost password or to download Cisco IOS software over the console port.

To use the ROM monitor, you must be using a terminal or PC that is connected to the router over the console port.

Timesaver Break (system interrupt) is always enabled for 60 seconds after the router reboots, regardless of whether it is set to on or off in the configuration register. During this 60-second window, you can break to the ROM monitor prompt by pressing the Break key.

Take these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted:

	Command	Purpose
Step 1	`Router>`**enable**	Enters privileged mode. If there is an enable password configured, enter the enable password to enter privileged EXEC mode.
Step 2	`Router#`**show version**	Displays the current register setting. Record the configuration register setting, which is typically 0x2102, so the register can be changed back to the original setting.
Step 3	`Router#`**configure terminal**	Enters global configuration mode.
Step 4	`Router(config)#`**config-reg 0x0**	Resets the configuration register.
Step 5	`Router(config)#`**exit**	Exits global configuration mode.

	Command	Purpose
Step 6	`Router#`**reload**	Reboots the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. Refer to the **boot** command in the "ROM Debug Commands" section.
	After the router reboots, it is in ROM monitor mode. To return the router to its original state, repeat the process, substituting the original value for the register.	

ROM Monitor Commands

Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 2>?
alias              set and display aliases command
boot               boot up an external process
break              set/show/clear the breakpoint
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
copy               Copy a file-copy [-b <buffer_size>] <src_file>
<dst_file>
delete             Delete file(s)-delete <filenames ...>
dir                List files in directories-dir <directory>
dis                display instruction stream
dnld               serial download a program module
format             Format a filesystem-format <filesystem>
frame              print out a selected stack frame
fsck               Check filesystem consistency-fsck <filesystem>
help               monitor builtin command help
history            monitor command history
meminfo            main memory information
mkdir              Create dir(s)-mkdir <dirnames ...>
more               Concatenate (type) file(s)-cat <filenames ...>
rename             Rename a file-rename <old_name> <new_name>
repeat             repeat a monitor command
reset              system reset
rmdir              Remove a directory
set                display the monitor variables
stack              produce a stack trace
sync               write monitor environment to NVRAM
sysret             print out info from last system return
tftpdnld           tftp image download
unalias            unset an alias
unset              unset a monitor variable
xmodem             x/ymodem image download
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, refer to the documentation for that product for information on how to send a Break command.

ROM Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or is halted. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

```
"xxx: kernel context state is invalid, can not proceed."
```

The following are ROM monitor debugging commands:

- **stack** or **k**—produce a stack trace; for example:

```
rommon 2> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**—displays processor context; for example:

```
rommon 2> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**—displays an individual stack frame.
- **sysret**—displays return information from the last booted system image. This information includes the reason for terminating the image, a stack dump of up to eight frames, and, if an exception is involved, the address where the exception occurred; for example:

```
rommon 3 > sysret
System Return Info:
count: 19,  reason: reset
pc:0x0,  error address: 0x0
Stack Trace:
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
rommon 4 >
```

- **meminfo**—displays size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of nonvolatile RAM (NVRAM); for example:

```
rommon 1> meminfo
Main memory size: 128 MB.
Available main memory starts at 0x1b000, size 130964KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 128KB
rommon 2 >
```

ROM Monitor Image Download by using TFTP

This section contains procedures for downloading software in ROM Monitor (ROMMON) mode by using the **tftpdnld** command.

Complete these steps to upgrade the ROMMON image from ROMMON mode.

Step 1 Download the ROMMON image from CCO, and place it on your Trivial File Transfer Protocol (TFTP) server.

Step 2 Place the router in ROMMON mode by sending a telnet **break** command during the router reboot sequence. The following prompt will be displayed, indicating entry into ROMMON mode:

```
rommon >
```

Step 3 In ROMMON mode, set the following parameters by typing the names followed by an equals sign as shown, and then typing a value for the parameter.

Table 18-1 describes the type of value to provide for each parameter.

Table 18-1 ROMMON Parameters and Values

Parameter	Value
IP_ADDRESS=	IP address of the router
IP_SUBNET_MASK=	Subnet mask of the router
DEFAULT_GATEWAY=	IP address of the router's default gateway
TFTP_SERVER=	IP address of the TFTP server on which the ROMMON image is located
TFTP_FILE=	The path and filename of the ROMMON image

Step 4 Verify the parameter settings by entering the **set** command. Correct any mistakes by reentering the parameter and value.

```
rommon> set
TFTP_CHECKSUM=0
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=1.6.0.1
TFTP_SERVER=223.255.254.254
IP_ADDRESS=1.6.97.20
TFTP_FILE=C3200_RM_ALT.srec.122-1r.XE2
```

Step 5 Upgrade the ROMMON image by entering the **tftpdnld -u** command. Sample output is shown below.

```
rommon >tftpdnld -u
IP_ADDRESS: 1.6.97.20
```

```
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 1.6.0.1
TFTP_SERVER: 223.255.254.254
TFTP_FILE: C3200_RM_ALT.srec.122-1r.XE2
WARNING: alternate copy of rommon exists, filename: C3200_RM_ALT.srec all existing data in
the alternate copy of rommon will be lost.
 Do you wish to continue? y/n:  [n]:
```

Step 6 Enter **y** to start the download. A series of exclamation points (!!!!!!) indicates that the image is downloading successfully. The router will reboot when the download is complete.

Note You may need to reset the router while in ROMMON mode by entering the **reset** command before entering the **tftpdnld** command. The router will prompt you to do this if needed. If prompted to reset the router, you must reset the router and then follow Step 2 through Step 6 to update the ROMMON image.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are only displayed on the console when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Cisco IOS Image Download from the Console Port

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. After download, the file is saved to the Flash memory.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the **ROM monitor** command.

Xmodem is used in disaster recovery situations where the router has no valid Cisco IOS software or bootflash image to boot from and hence, only boots up in ROMmon. This procedure can also be used where there are no Trivial File Transfer Protocol (TFTP) servers or network connections, and a direct PC connection (or through a modem connection) to the router's console is the only viable option. Because this procedure relies on the console speed of the router and the serial port of the PC, it can take a long time to download an image.

Configure Windows HyperTerminal for 8-N-1 at 9600 bps and connect your PC's serial port to the console port of the router. Once connected, you need to get into the ROMmon prompt (rommon 1>). Typically, if the Cisco IOS software image and bootflash image are both corrupt, the router only comes up in ROMmon mode. If the former is not true and you need to get into the ROMmon prompt, change the configuration register (typically 0x2102 as given by show version) to 0x0 as described in the "Access ROM Monitor Mode" section.

Console port PC settings are also described in the "Terminal Configuration" section of the "Cisco 3200 Series Mobile Access Router Interfaces" chapter.

Follow the steps below to run Xmodem:

Step 1 Move the image file to the local drive where the Xmodem will execute.

Step 2 Launch the terminal emulation application, such as HyperTerminal.

Note You might have to reset the registry so the router boots from rommon.

Step 3 Enter the **xmodem** command.

Following is the syntax and descriptions for the **xmodem** console download command. For example:

```
rommon 1 >xmodem c3220-i11k9-mz.123-2.XA2.bin
```

The router displays the message:

```
Do you wish to continue? y/n  [n]:  y
```

Step 4 Type **y** and press **Enter**. The system displays a message indicating that it is ready to receive the file:

```
Ready to receive file c3220-i11k9-mz.123-2.XA2.bin
```

Step 5 Click **Transfer>Send File**. The **Send File** window displays.

Step 6 Type the file name in the **Filename** field or use the **Browse** button to select the file from the Explorer.

Step 7 Select the protocol, typically Xmodem, from the **Protocol** drop-down list.

Step 8 Click **Send**. The **Xmodem** file send window displays. Note that it might take a few seconds before the file transfer begins.

Download Errors

The following error displays if you are try to download a corrupt file, a file that is not an executable file, or a file that is not acceptable to the router. For example, if you try to download a Cisco 3250 base IOS image to a Cisco 3200 Series router.

```
Ready to receive file c3200-i11-mz.122-15.ZL.bin
BB0Download Complete!

ERR:File not a valid executable
rommon 36 >
```

xmodem Syntax

The syntax for the **xmodem** command is as follows:

```
xmodem [-ucyrx] destination_file_name
```

u	(Optional) Performs and upgrade of the ROMMON. System reboots after the file is upgraded.
c	(Optional) Performs the download using 16-bit cyclic redundancy check (CRC-16) error checking to validate packets. Default is 8-bit CRC.
y	(Optional) Sets the router to perform the download using Ymodem protocol. Default is Xmodem protocol. The protocols differ as follows: • Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size. • Ymodem uses (CRC)-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.
r	(Optional) Image is loaded into DRAM for execution. Default is to load the image into Flash memory.
x	(Optional) Image is loaded into DRAM without being executed.
destination_file_name	The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

WMIC Image Update over FESMIC Port

This section describes the procedure for updating the software image on a MARC and WMIC over wired connection to a TFTP server through a port on FESMIC. It is also possible to update the software image on the WMIC by using a wireless connection; however, it is not described here.

To download the image, do the following:

Step 1 Add following to the configuration on the MARC. The IP addresses used are for illustration only and should be replaced by the IP addresses used in your configuration.

```
ip dhcp pool fa0
   network 10.0.0.0 255.0.0.0 (network <network addr of Fa0>)
   default-router 10.0.0.1 (default-router <ip addr of fa0/0)
ip dhcp pool vlan1
   network 30.0.0.0 255.0.0.0 (network <network addr of Vlan1>)
   default-router 30.0.0.1 (default-router <ip addr ofVlan1)
no spanning-tree vlan 1
no spanning-tree vlan 2
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0 (ip address <ip addr>)
 ip nat inside
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
interface FastEthernet1/1
 switchport access vlan 2
 no ip address
interface Vlan1
 ip address 30.0.0.1 255.0.0.0 (ip address <ip addr>)
 ip nat inside
interface Vlan2
 ip address 1.7.43.9 255.255.0.0  (ip address <ip addr of TFTP network>)
 ip nat outside
```

```
ip nat inside source list 100 interface Vlan2 overload
ip route 223.255.254.0 255.255.255.0 Vlan2 (ip route <TFTP server network> Vlan2)
access-list 100 permit ip any any
```

Procedure:

Step 2 Use default configuration on Cisco 3201 WMIC. By default, the Cisco 3201 WMIC uses DHCP to acquire an IP address for Bridge Group Virtual Interface (BVI). The Cisco 3201 WMIC Workgroup Bridge BVI IP address is 10.0.0.2 and Cisco 3201 WMIC Root Bridge BVI IP address is 30.0.0.2. These are the Telnet addresses.

Step 3 Log-in into the Cisco 3251 through its console port and download image.

Step 4 Telnet into the WMIC after log-in into the MARC through its console port and then download image.

Flash and NVRAM File Management

The router uses a random access file system. It is not necessary to erase an entire file space to reclaim memory held by deleted files, because the random access file system has a hierarchical directory structure that allows you to delete individual files. When the file is deleted, the memory space is freed. In contrast, the low end system (LES) file system used by other platforms, such Cisco 2500 Series routers and Cisco 5200 Series routers, has no provision for reclaiming the space from deleted files.

NVRAM is the segment of Flash memory reserved exclusively by Cisco IOS to store the configuration files for the router. When an Cisco IOS image is loaded, it reads the configuration files to determine which interfaces to bring up and what kind of configurations to use.

Delete Configuration Files

To erase a configuration file, use the **delete nvram:config** command:

```
Router#delete nvram:config
Delete filename [config]? filename
Delete nvram:config? [confirm] filename
Router#
```

or if the file is in Flash (the device name is optional)

```
Router#delete startup-config
Delete filename [startup-config]? filename
Delete flash:startup-config? [confirm] filename
Router#
```

Erase the Flash File System

To delete all files in Flash, use the **erase flash:** command:

```
Router#erase flash:
Erasing the flash filesystem will remove all files! Continue? [confirm]
flashfs[10]: 0 files, 1 directories
flashfs[10]: 0 orphaned files, 0 orphaned directories
flashfs[10]: Total bytes: 31739904
flashfs[10]: Bytes used: 4096
flashfs[10]: Bytes available: 31735808
flashfs[10]: flashfs fsck took 5 seconds.
Erase of flash: complete
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
copy	Duplicates a file.
delete	Deletes a file.

Command	Description
dir	Displays a list of files.
more	Continues a list that has been paused.
rename	Changes the name of a file.
verify	Verifies the checksum of a file before using it.
cd	Changes the default directory or file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.
format	Formats a file system.
fsck	Validates a file system.
rmdir	Removes a directory.

Mobile IP Debug

This section shows normal operating debugs and configurations of Mobile IP.

Note TLV stands for Type, Length, Value. It is the template used in registration request and reply messages. See RFC 2002 for more information.

Debug Commands for Troubleshooting

The following debug commands are useful in troubleshooting Mobile IP clients:

- debug arp
- debug ip icmp
- debug ipmobile host
- debug ip mobile
- debug ip packet detail

The **debug arp** command shows you the mobile node ARPs on the local subnet. It can also help determine if the mobile node is causing a **MobileIP: FastEthernet1/0 add 10.0.150.200 rejected** error message or if the interface does not have IRDP configured.

The **debug ip icmp** command shows you the mobile node solicitations and the replies. The **debug ip mobile advertisements** command only shows you the foreign agent replies to solicitations from the Mobile IP client or unsolicited advertisements, not the actual Mobile IP client solicitations.

The **debug ip mobile** command is a combination of the **debug ip mobile host** and **debug ip mobile advertisements** commands. The **debug ip mobile host** command shows all of the normal Mobile IP debugs except for the IRDP replies to solicitations and the skip2TLV messages as the home agent or foreign agent searches the request or the reply for information.

The **debug ip packet detail** command is used with an access list and shows you all the Mobile IP packets at the foreign agent since they are all still process switched.

Good Registration from a Mobile Client on a Foreign Network

These debug results show what occurs during a normal *good* registration. In these examples:

- The Mobile IP client is coming up from a power on state.
- The mobile node ARPs in the beginning against the RFC and the router rejects the IP address.
- The Mobile IP client registration request is rejected the first time it tries to register with the home agent because its clock is too far out of synchronization with the home agent clock.

The home agent registration reply contains the offset the Mobile IP client will use for the next registration request. The mobile node registers successfully on the second attempt, after adjusting its timestamp with the offset sent by the home agent.

On the Foreign Agent:

```
*Mar 16 22:09:15:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27773,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:15: Care-of address: 192.1.1.1
*Mar 16 22:09:15: ICMP: src=192.1.1.1, dst=255.255.255.255, irdp advertisement sent
*Mar 16 22:09:15: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:15: IRDP: address=192.1.1.1 preference=0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:18: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:19: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:20: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
*Mar 16 22:09:20: ICMP: rdp solicit rcvd type 10, code 0, from 10.0.150.200
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:20: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
*Mar 16 22:09:20:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27774,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:20: Care-of address: 192.1.1.1
*Mar 16 22:09:20: ICMP: src=192.1.1.1, dst=10.0.150.200, irdp advertisement sent
*Mar 16 22:09:20: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:20: IRDP: address=192.1.1.1 preference=0
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:20: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received registration id mismatch (133) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:21: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
```

```
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received accept (0) reply for MN 10.0.150.200 on FastEthernet0/0 using HA
10.0.150.6 lifetime 180
MobileIP: Reply in for MN 10.0.150.200, accepted
MobileIP: Update visitor table for MN 10.0.150.200
MobileIP: Tunnel0 (IP/IP) created with src 192.1.1.1 dst 10.0.150.6
MobileIP: ARP entry for MN 10.0.150.200 inserted
MobileIP: Visitor timer started for MN 10.0.150.200, lifetime 180
MobileIP: FA dequeued MN 10.0.150.200 from register table
MobileIP: MN 10.0.150.200 visiting on FastEthernet1/0
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: swif coming up Tunnel0
```

Advertisements are sent out.

```
*Mar 16 22:09:24:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27773,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:24: Care-of address: 192.1.1.1
*Mar 16 22:09:24: ICMP: src=192.1.1.1, dst=255.255.255.255, irdp advertisement sent
*Mar 16 22:09:24: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:24: IRDP: address=192.1.1.1 preference=0
```

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Identification field has timestamp 240175185 secs greater than our current time
03/16/93 03:48:14 (> allowed 255 secs) for MN 10.0.150.200
*Mar 15 19:48:14: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode registration id mismatch (133), reason Bad identifier (3)
MobileIP: HA rejects registration for MN 10.0.150.200 - registration id mismatch (133)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 requested broadcast support, but disabled locally
MobileIP: Mobility binding for MN 10.0.150.200 created
MobileIP: Tunnel0 (IP/IP) created with src 10.0.150.6 dst 192.1.1.1
MobileIP: Roam timer started for MN 10.0.150.200, lifetime 180
MobileIP: MN 10.0.150.200 is now roaming
MobileIP: Insert host route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: HA accepts registration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
MobileIP: swif coming up Tunnel0
```

Deregistration When a Mobile Node Returns to the Home Network

This example shows the mobile node deregistration when it arrives on its home network. The IKV mobile client repeats the deregistration process 3 times.

On the Home Agent:

```
*Mar  1 03:31:51: IP: s=10.0.150.200 (FastEthernet0/0), d=255.255.255.255, len 28, rcvd 0
*Mar  1 03:31:51:     ICMP type=10, code=0
*Mar  1 03:31:54:
MobileIP: Agent advertisement sent out FastEthernet0/0: type=16, len=6, seq=0,
lifetime=36000, flags=0x2400(rbHfmGv-rsv-),
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=255.255.255.255 (FastEthernet0/0), len 44,
sending broad/multicast
*Mar  1 03:31:54:     ICMP type=9, code=0
*Mar  1 03:31:54: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:31:54:     UDP src=1050, dst=434
MobileIP: HA 92 received deregistration for MN 10.0.150.200 on FastEthernet0/0 using COA
10.0.150.200 HA 10.0.150.6 lifetime 0 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: HA accepts deregistration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200, len 70, cef process switched
*Mar  1 03:31:54:     UDP src=434, dst=1050
*Mar  1 03:31:54: IP ARP: creating incomplete entry for IP address: 10.0.150.200 interface
FastEthernet0/0
*Mar  1 03:31:54: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.200 0000.0000.0000 FastEthernet0/0
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
sending
*Mar  1 03:31:54:     UDP src=434, dst=1050
*Mar  1 03:31:54: IP ARP throttled out the ARP Request for 10.0.150.200
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
encapsulation failed
*Mar  1 03:31:54:     UDP src=434, dst=1050
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.200
*Mar  1 03:31:54: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
*Mar  1 03:32:01: IP: s=10.0.150.200 (FastEthernet0/0), d=255.255.255.255, len 28, rcvd 0
*Mar  1 03:32:01:     ICMP type=10, code=0
*Mar  1 03:32:01: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
```

Transition from the Home Network to a Foreign Network

This debug example shows the mobile node transitioning from the home network to a foreign network. For the mobile node to send a registration request, it must first be alerted that it has changed subnets. It does this by waiting for the advertisement timeout to expire, and then sending a solicitation.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 requested broadcast support, but disabled locally
MobileIP: Mobility binding for MN 10.0.150.200 created
```

```
MobileIP: Tunnel0 (IP/IP) created with src 10.0.150.6 dst 192.1.1.1
MobileIP: Roam timer started for MN 10.0.150.200, lifetime 180
MobileIP: MN 10.0.150.200 is now roaming
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
MobileIP: Gratuitous ARPs sent for MN 10.0.150.200 MAC 0002.4bb0.ecb0
MobileIP: Insert host route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: HA accepts registration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:52:31: IP ARP: creating incomplete entry for IP address: 10.0.150.5 interface
FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.5 0000.0000.0000 FastEthernet0/0
*Mar  1 03:52:31: IP ARP throttled out the ARP Request for 10.0.150.5
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
*Mar  1 03:52:31: IP ARP: rcvd rep src 10.0.150.5 0010.7bb2.8d80, dst 10.0.150.6
FastEthernet0/0
MobileIP: swif coming up Tunnel0
```

Transition from a Foreign Network to the Home Network

This debug example shows the mobile node transitioning from a foreign network to a home network.

On the Home Agent:

```
*Mar  1 03:56:35: IP: s=10.0.150.6 (local), d=255.255.255.255 (FastEthernet0/0), len 44,
sending broad/multicast
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:56:35:     UDP src=1050, dst=434
MobileIP: HA 92 received deregistration for MN 10.0.150.200 on FastEthernet0/0 using COA
10.0.150.200 HA 10.0.150.6 lifetime 0 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Delete tunnel route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: Deleted Tunnel0 src 10.0.150.6 dest 192.1.1.1
*Mar  1 03:56:35: ip_mobile_query
MobileIP: HA route maint started with index 0
MobileIP: MN 10.0.150.200 back home
*Mar  1 03:56:35: IP ARP: creating incomplete entry for IP address: 10.0.150.200 interface
FastEthernet0/0
*Mar  1 03:56:35: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.200 0000.0000.0000 FastEthernet0/0
*Mar  1 03:56:35: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
MobileIP: Get ARP entry for MN 10.0.150.200 succeeded
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
MobileIP: Gratuitous ARPs sent for MN 10.0.150.200 MAC 0010.a403.1357
MobileIP: HA accepts deregistration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:56:36: IP: s=10.0.150.6 (local), d=10.0.150.200, len 70, cef process switched
```

```
*Mar  1 03:56:36:     UDP src=434, dst=1050
*Mar  1 03:56:36: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
sending
*Mar  1 03:56:36:     UDP src=434, dst=1050
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.200
*Mar  1 03:56:36: IP ARP: rcvd req src 10.0.150.200 0010.a403.1357, dst 0.0.0.0
FastEthernet0/0
*Mar  1 03:56:36: IP ARP: rcvd req src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.6 0002.4bb0.ecb0,
                dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
FastEthernet0/0
```

Verifying Operation

Verify that the foreign agent is sending agent advertisements.

Turn on **debug ip mobile advertise** on the foreign agent. The following messages should be displayed periodically (based on *number* in the **ip irdp max** command).

```
00:08:11: MobileIP: Agent advertisement sent out Ethernet3/1: type=16, len=10, seq=3,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
00:08:11: Care-of address: 27.0.0.12
```

If not, make sure configuration for interface and care-of address is correct.

Verify the mobile access router receives agent advertisements.

Turn on **debug ip icmp** on mobile access router. The following message should be displayed periodically.

```
2w2d: ICMP: rdp advert rcvd type 9, code 0, from 27.0.0.12
```

Make sure interface receiving agent advertisement is configured for roaming. Enter the **show ip mobile router interface** command to display interface information.

Verify the mobile access router learns about the foreign agent.

Enter the **show ip mobile router agent** command on the mobile access router to display foreign agent information.

Verify mobile access router registration.

Turn on **debug ip mobile router** on the mobile access router. The following messages should be displayed.

```
MobileRouter: New FA 27.0.0.12 coa 27.0.0.12 int Ethernet0/1 MAC 0050.50c1.c855
2w2d: MobileRouter: Register reason: isolated
2w2d: MobileRouter: Snd reg request agent 27.0.0.12 coa 27.0.0.12 home 9.0.0.1 ha 29.0.0.4
lifetime 36000 int Ethernet0/1 flag sbdmgvt cnt 0 id B496B69C.55E77974
2w2d: MobileRouter: Status Isolated -> Pending
```

Enter the **show ip mobile router registration** command on mobile access router to display registration information. When mobile access router is registered, the **show ip mobile router registration** command displays when request was last accepted and the **show ip mobile router** command displays the status of the register.

If the mobile access router is not registered, turn on **debug ip mobile host** on the home agent to see registration debugging messages. Make sure the SPI and key are same on both the mobile access router and the home agent by using the **show ip mobile secure home-agent** and **show ip mobile secure host** commands. Make sure the home agent knows how to reach foreign agent by using the **show ip route** command, which displays the route to the care-of address.

Turn on **debug ip mobile host** on both the foreign agent and the home agent to see Mobile IP activities.

Enter the **show ip mobile router** command to display mobile access router information.

Turn on **debug tunnel** on the home agent, the foreign agent, and the mobile access router. For packets that are process switched, the following messages are displayed.

```
00:55:33: Tunnel0: to decaps IP/IP packet 29.0.0.4->27.0.0.12 (len=140, ttl=254)
00:55:33: Tunnel0: decapsulated IP/IP packet 29.0.0.4->9.0.0.1 (len=120 ttl=255)
```

For packets that are fast switched, use the **show ip cache** command to display the cache entries.

Error Codes

This section provides a summary of error codes returned in registration replies from the home agent. Some configuration errors on the home agent do not return a registration reply and so no code is sent to the foreign agent or mobile node. One of these types of errors occurs when the mobile node does not have a security association (SA). In this case, the home agent registers an error and drops the packet. The best place to debug general problems is on the home agent.

Error Code	Description
131	Security Association mismatch, such as bad password, bad security parameter index (SPI)
133	Time clocks not synchronized (mismatched id)
128	Configuration error on HA

Foreign Agent Registration Error Codes

Code	Description
64	* reason unspecified *
65	* administratively prohibited *
66	* insufficient resource *
67	* MN failed authentication *
68	* HA failed authentication *
69	* requested lifetime too long *
70	* poorly formed request *
71	* poorly formed reply *
72	* requested encapsulation unavailable *
73	* requested Van Jacobson compression unavailable *
74	* reverse tunnel unsupported *

75	* reverse tunnel mode only *
80	* unreachable base value *
80	* home network unreachable *
81	* HA host unreachable (not used, but in RFC2002)*
82	* HA port unreachable (not used, but in RFC2002)*
83	* HA unreachable (not used, but in RFC2002)*

Home Agent Registration Error Codes

Code	Description
128	* reason unspecified *
129	* administrative prohibited *
130	* insufficient resource *
131	* MN failed authentication *
132	* FA failed authentication *
133	* registration identification mismatched *
134	* poorly formed request *
135	* too many simultaneous bindings *
136	* unknown HA address *
137	* reverse tunnel unavailable *
138	* reverse tunnel mode only *
139	* unsupported encapsulation *
140	* active HA failed authentication (not in RFC2002)*

Debug Troubleshooting Scenarios

This section describes the following specific problems:

- Bad Password
- Bad SPI
- No IRDP on Foreign Agent Interface
- No IRDP on Home Agent Interface
- Time Clocks Not Synchronized on Mobile Node and Home Agent (usually not a problem)
- Missing ip mobile virtual-network Command on the Home Agent
- Mobile Node Is Not On Line
- No Security Association for the Mobile Node on the Home Agent (a home agent configuration error)

Bad Password

The debug messages in this example show what happens on the home agent and foreign agent when either the home agent or the Mobile IP client is configured with an incorrect password. The passwords on the home agent and Mobile IP client must match.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - invalid authenticator for MN 10.0.150.200
*Mar  1 03:10:32: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode MN failed authentication (131), reason Bad authenticator (2)
MobileIP: HA rejects registration for MN 10.0.150.200 - MN failed authentication (131)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3D04EAC end 3D04EC2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received MN failed authentication (131) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3D04EA8 end 3D04EBE
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
```

Bad SPI

This debug example shows when the SPI specified on the home agent does not match the SPI specified on the Mobile IP client.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36BAC end FA36BC2
MobileIP: Skip2TLV look for type 32, addr start FA36BC2 end FA36BC2
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - SPI 100 for MN 10.0.150.200 is not configured
*Mar  1 03:05:08: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode MN failed authentication (131), reason Bad SPI (4)
MobileIP: HA rejects registration for MN 10.0.150.200 - MN failed authentication (131)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 101) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
*Mar  2 05:25:19: IP: s=10.0.150.200 (FastEthernet1/0), d=192.1.1.1 (FastEthernet1/0), len
74, rcvd 3
*Mar  2 05:25:19:     UDP src=1050, dst=434
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B01A0C end 3B01A22
*Mar  2 05:25:19: IP: s=10.0.150.5 (local), d=10.0.150.6, len 74, cef process switched
*Mar  2 05:25:19:     UDP src=434, dst=434
*Mar  2 05:25:19: IP: s=10.0.150.5 (local), d=10.0.150.6 (FastEthernet0/0), len 74,
sending
*Mar  2 05:25:19:     UDP src=434, dst=434
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
*Mar  2 05:25:19: IP: s=10.0.150.6 (FastEthernet0/0), d=10.0.150.5 (FastEthernet0/0), len
70, rcvd 3
*Mar  2 05:25:19:     UDP src=434, dst=434
MobileIP: FA received MN failed authentication (131) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01A08 end 3B01A1E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
```

No IRDP on Foreign Agent Interface

This debug example shows where ICMP Router Discovery Protocol (IRDP) is not configured on the foreign agent interface. It shows the ARP process reacting to the mobile nodes address when it tries to put it in the ARP table. The router adds the mobile node address in the ARP table when it sends a registration request or an ip IRDP solicitation. In either case, IRPD must be enabled on the foreign agent interface.

On the Foreign Agent:

```
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
 (repeated …)
```

No IRDP on Home Agent Interface

This debug example shows where IRDP is not configured on the home agent interface. On the home agent, the interface continues to receive solicitations from the Mobile IP client. Unlike the foreign agent, there are no ARPing errors because the host is on the correct subnet.

On the Home Agent:

```
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
```

Time Clocks Not Synchronized on Mobile Node and Home Agent

This debug example shows the clock of the Mobile IP client is not within the specified variance of the home agent clock. The identification field in the registration reply holds the clock of the mobile node when the clock does not match the home agent clock. The registration request is rejected and the home agent sends a reply with the offset between the clocks on the mobile nodes and home agent clock. The mobile node corrects its timestamp in the next registration request, so it matches the home agent clock.

On the Home Agent:

```
MobileIP: HA 91 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
193.1.1.1 HA 10.1.1.1 lifetime 300 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D06
MobileIP: Skip2TLV look 32 != type 200, addr FA36CEC end FA36D06
MobileIP: Skip2TLV skipping 2
MobileIP: Skip2TLV look for type 32, addr start FA36D06 end FA36D06
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Identification field 970198610 has timestamp 1969734999 secs less than our
current time 03/01/93 00:13:29 2939933609 (< allowed 255 secs) for MN 10.0.150.200
*Feb 28 16:13:29: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode registration id mismatch (133), reason Bad identifier (3)
MobileIP: HA rejects registration for MN 10.0.150.200 - registration id mismatch (133)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 172.1.1.2
```

On the Foreign Agent:

```
*Feb 28 16:07:17:
MobileIP: Agent advertisement sent out FastEthernet0/1: type=16, len=10, seq=38,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Feb 28 16:07:17: Care-of address: 193.1.1.1
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet0/1 using COA
193.1.1.1 HA 10.1.1.1 lifetime 300 options sbdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3CB5CEC end 3CB5D06
MobileIP: Skip2TLV look 32 != type 200, addr 3CB5CEC end 3CB5D06
MobileIP: Skip2TLV skipping 2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.1.1.1
MobileIP: FA received registration id mismatch (133) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.1.1.1 lifetime 300
MobileIP: Skip2TLV look for type 32, addr start 3CB5CE8 end 3CB5CFE
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
*Mar  1 03:56:36: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
FastEthernet0/0
```

Missing ip mobile virtual-network Command on the Home Agent

This section shows an example of a configuration error on the home agent. Other configuration errors return the same code (128). Some errors cause the home agent not to respond with a registration reply. One of those is a missing security association for the mobile node.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.148.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.148.200 - authenticating MN 10.0.148.200 using SPI 100
MobileIP: MN 10.0.148.200 - authenticated MN 10.0.148.200 using SPI 100
MobileIP: Request from MN 10.0.148.200 denied, no virtual network 10.0.148.0
MobileIP: HA rejects registration for MN 10.0.148.200 - reason unspecified (128)
MobileIP: MN 10.0.148.200 - MH auth ext added (SPI 100) to MN 10.0.148.200
MobileIP: MN 10.0.148.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
*Mar 16 21:48:37: ICMP: rdp solicit rcvd type 10, code 0, from 10.0.148.200
MobileIP: FastEthernet1/0 glean 10.0.148.200 accepted
*Mar 16 21:48:37:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27734,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 21:48:37: Care-of address: 192.1.1.1
*Mar 16 21:48:37: ICMP: src=192.1.1.1, dst=10.0.148.200, irdp advertisement sent
*Mar 16 21:48:37: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 21:48:37: IRDP: address=192.1.1.1 preference=0
MobileIP: FA received registration for MN 10.0.148.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.148.200 accepted
MobileIP: FA queued MN 10.0.148.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.148.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
MobileIP: FA forwarded registration for MN 10.0.148.200 to HA 10.0.150.6
MobileIP: FA received reason unspecified (128) reply for MN 10.0.148.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.148.200 using src 10.0.148.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.148.200 from register table
```

Mobile Node Is Not On Line

In this example, the mobile node is not online.

On the Home Agent:

```
MobileIP: MN 10.0.148.1 is offline, icmp unreachable sent to sender 10.0.150.5
*Mar 16 20:31:59: ICMP: dst (10.0.148.1) host unreachable sent to 10.0.150.5
```

No Security Association for the Mobile Node on the Home Agent

In this example, nothing is sent back to a foreign agent, no registration reply, no ICMP unreachable. The registration request is completely ignored.

On the Home Agent:

```
MobileIP: HA 91 received registration for MN 10.0.148.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: MN 10.0.148.200 SA is not configured, request ignored
*Feb 28 16:02:20: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.148.200 -
errcode MN failed authentication (131), reason No mobility security association (1)
```

Configuration Register Modification

The virtual configuration register is in nonvolatile RAM (NVRAM) and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software.

Table 18-2 shows the software configuration bit descriptions.

Table 18-2 Software Configuration Bit Descriptions

Bit No.	Hex	Description
00-03	0x0000-0x000F	Boot Field (see Table 18-3)
06	0x0040	Ignore NVM contents
07	0x0080	OEM bit enabled
08	0x0100	Break disabled
10	0x0400	IP broadcast with all zeros
11-12	0x0800-0x1000	Console line speed
13	0x2000	Boot default ROM software if network boot fails
14	0x4000	IP broadcasts do not have net numbers
15	0x8000	Enable diagnostic messages and ignore NVM contents

Table 18-3 shows the boot field register bits.

Table 18-3 Explanation of Boot Field (Configuration Register Bits 00-03)

Boot Field	Meaning
00	Stays at the system bootstrap prompt
01	Boots system image on EPROM
02-F	Specifies a default netboot filename Enables boot system commands that override default netboot filename[1]

1. Values of the boot field are 2-15 in the form cisco<n>-processor_name, where 2 < n < 15.

The value is always interpreted as hexadecimal. Entering **confreg** without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

In either case, the new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

To change the virtual configuration register from the ROM monitor, enter **confreg** or enter the new value of the register in hexadecimal.

The following display shows an example of entering the **confreg** command:

```
rommon 2> confreg

Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable diagnostic mode? y/n  [n]:  y
enable use net in IP bcast address? y/n  [n]:
enable load rom after netboot fails? y/n  [n]:
enable use all zero broadcast? y/n  [n]:
enable break/abort has effect? y/n  [n]:
enable ignore system config info? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:

You must reset or power cycle for new config to take effect
```

Password Recovery

This section describes how to recover a password that you configured with the **enable** command (enable password) on the Cisco 3200 Series router.

Note You can recover a lost enable password, but not a password that you configured with the **enable secret** command (enable secret password). This password is encrypted and must be replaced with a new enable secret password. See the "Hot Tips" section on Cisco Connection Online (CCO) for information on replacing enable secret passwords.

Follow these steps to recover a lost enable password:

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the Console port. For more information, see the "Terminal Configuration" section of the "Cisco 3200 Series Mobile Access Router Interfaces" chapter.

Step 2 Configure the terminal at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 Reboot the router.

Step 4 From user EXEC mode, display the existing configuration register value:

```
Router> show version
```

Step 5 Record the setting of the configuration register. The setting is usually 0x2102 or 0x102.

Step 6 Record the break setting.

- Break enabled—bit 8 is set to 0.
- Break disabled (default setting)—bit 8 is set to 1.

Note To enable break, enter the **config-register 0x01** global configuration command. The bit settings are described in Table 18-2.

Step 7 Turn off the power to the router and then turn it back on.

Step 8 Press **Break** on the terminal keyboard within 60 seconds of the power-up to put the router into ROMMON. The terminal displays the following prompt:

```
rommon 1>
```

Step 9 Reset the configuration register:

```
rommon 1> confreg 0x2142
```

Step 10 Initialize the router:

```
rommon 2> reset
```

The router reboots but ignores its saved configuration.

```
--- System Configuration Dialog ---
```

Step 11 Enter **no** in response to the prompts until the following message is displayed:

```
Press RETURN to get started!
```

Step 12 Press **Return**. The following prompt appears:

```
router>
```

Step 13 Enter privileged EXEC mode:

```
router> enable
```

The prompt changes to the privileged EXEC prompt:

```
router#
```

Step 14 Type **configure memory** or **copy startup-config running-config** to copy the nonvolatile RAM (NVRAM) into memory. Do not type configure terminal.

Step 15 Type **write terminal** or **show running-config**.

The **show running-config** and **write terminal** commands show the configuration of the router. In this configuration you see under all the interfaces the shutdown command, which means all interfaces are currently shutdown. Also, you can see the passwords (enable password, enable secret, vty, console passwords, and so on) either in encrypted or unencrypted format. The unencrypted passwords can be re-used, the encrypted ones will have to be changed with a new one.

Step 16 Type **configure terminal**.

```
router# configure terminal
hostname(config)#
```

Step 17 Type **enable secret** *password* to change the enable secret password, for example:

```
hostname(config)#enable secret cisco
```

Step 18 Issue the **no shutdown** command on every interface that is used. If you issue a **show ip interface brief** command, every interface that you want to use should be "up up".

Step 19 Type config-register 0x2102, or the value that you recorded in Step 5.

```
router# config-register value
```

Step 20 Press **Ctrl-Z** to exit configuration mode.

Step 21 Type **write memory** or **copy running-config startup-config** to commit the changes.

Step 22 Reboot the router, and enter the recovered password.

Numerics

802.11b/g An IEEE specification for a wireless LAN airlink.

A

agent advertisement An advertisement message constructed by attachment of a special extension to a router advertisement message.

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

agent solicitation A request for an agent advertisement.

B

binding information Binding information contains the entries in the mobility binding table.

binding information reply Active HA replies with all binding information to standby HA when request received.

binding information reply acknowledgement The peer home agent acknowledges that it has received the requested binding information.

binding information request The HA sends a binding information request to its peer to retrieve all mobility bindings for a specified HA address.

binding update A binding update contains the information in a mobile node's registration request. The HA sends the update to its peer after accepting a registration.

C

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

collocated care-of address An IP address temporarily assigned to the interface of the mobile node. A collocated care-of address represents the current position of the mobile node on the foreign network and can be used by only one mobile node at a time.

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

F

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

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

G

Generic routing encapsulation (GRE) A generic encapsulation procedure, defined in RFC 1701, that was developed prior to the development of Mobile IP.

H

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

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

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

HSRP group address The virtual IP address of the HSRP group.

I

inform An SNMP trap message that includes a delivery confirmation request. See “trap.”

L

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

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

loopback address A special IP number that is designated for the software loopback interface of a machine. The loopback interface has no hardware associated with it, and it is not physically connected to a network. This allows testing of software even if a physical device goes down.

loopback interface A software function that emulates many of the functions of a real interface.The loopback interface has no hardware associated with it, and it is not physically connected to a network.

Internet Control Message Protocol (ICMP) Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

M

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

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

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

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

mobility agent A Home Agent or a Foreign Agent.

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

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

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

N

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

node A host or router.

P

PC104+ A compact version of PC, PC/AT, and PCI bus.

peer HA Active HA and standby HA are peers to each other.

physical network Physical infrastructure of a network, for example, cables and wires.

R

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

roaming interface An interface used by the Mobile Router to detect Foreign Agents and Home Agents while roaming. Registration and traffic occur on the interface.

RRP Mobile IP Registration Reply

RRQ Mobile IP Registration Request

S

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

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

T

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

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

V

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

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

visitor list The list of mobile nodes visiting a Foreign Agent.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z