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

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

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

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

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

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

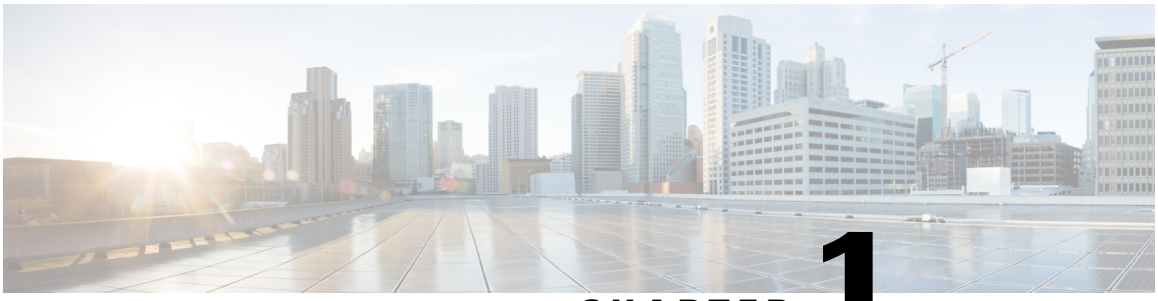
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Cisco Mobile Networks

Feature History

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

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

Finding Feature Information

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

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

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

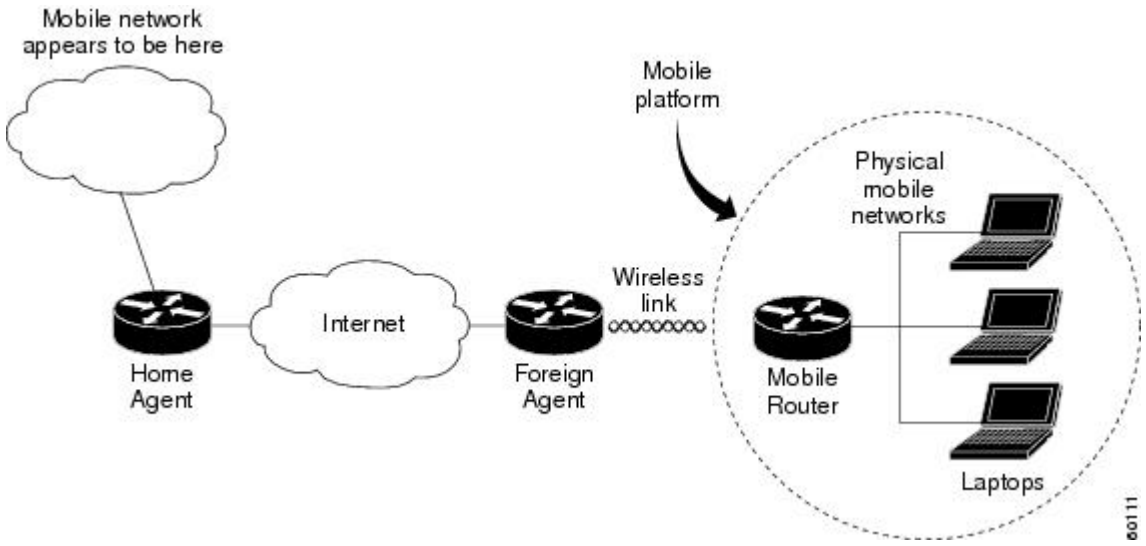
Feature Overview

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

Mobile IP, as defined in standard RFC 3344, provides the architecture that enables the mobile router to connect back to its home network. Mobile IP allows a device to roam while appearing to a user to be at its home network. Such a device is called a mobile node. A mobile node is a node--for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone--that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain ongoing communications while using the same IP address. There is no need for any changes to applications because the solution is at the network layer, which provides the transparent network mobility.

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

Figure 1: Cisco Mobile Network Components and Relationships



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

These destination devices can be mobile nodes running mobile IP client software or nodes without the software. The mobile router eliminates the need for a mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The mobile router "hides" the IP roaming from the local IP nodes so that the

local nodes appear to be directly attached to the home network. See the Mobile Router, on page 4 section later in this document for more details on how the mobile router operates.

A home agent is a router on the home network of the mobile router that provides the anchoring point for the mobile networks. The home agent maintains an association between the home IP address of the mobile router and its *care-of address* , which is the current location of the mobile router on a foreign or visited network. The home agent is responsible for keeping track of where the mobile router roams and tunneling packets to the current location of the mobile network. The home agent also injects the mobile networks into its forwarding table. See the Home Agent, on page 5 section later in this document for more details on how the home agent operates.

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

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

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

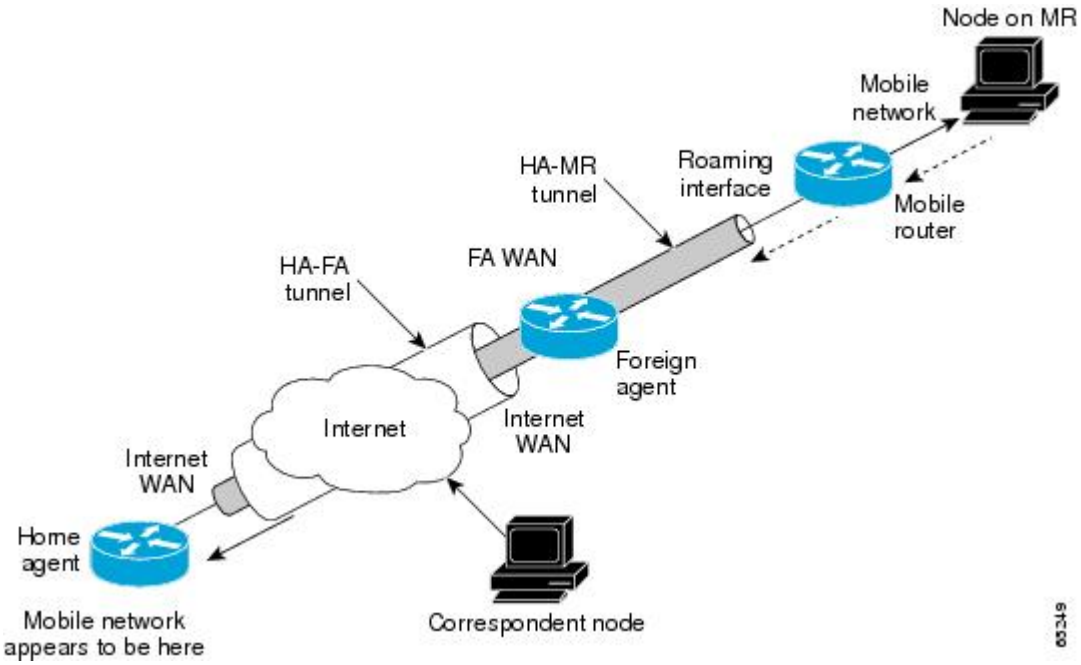
Cisco IOS Release 12.2(4)T implements mobile node MIB groups from the RFC2006-MIB for the monitoring and management of Cisco Mobile Network activity. Data from managed objects is returned through the use of the **show** commands described in this document, or can be retrieved from a Network Management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

Primary Components of Cisco Mobile Networks

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

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

Figure 2: Routing Within the Cisco Mobile Network



Mobile Router

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

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

Agent Discovery

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

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

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

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

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

Registration

The mobile router is configured with its home address, the IP address or addresses of its home agents, and the mobility security association of its home agent. There is a shared key between the mobile router and the home agent for authentication, as discussed in the Security for Mobile Networks, on page 6 section later in this document. The mobile router uses this information along with the information that it learns from the foreign agent advertisements to form a registration request.

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

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

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

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

Routing

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

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

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

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

Home Agent

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

Registration

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

The home agent also creates a *mobility binding table* that maps the home IP address of the mobile router to the current care-of address of the mobile router. An entry in this table is called a *mobility binding* . The main purpose of registration is to create, modify, or delete the mobility binding of a mobile router (or mobile node) at its home agent.

The home agent processes registration requests from the mobile router in the same way that it does with the mobile node. The only difference is that an additional tunnel is created to the mobile router. Thus, packets destined to the mobile networks are encapsulated twice, as discussed in the Routing, on page 6 section that follows. The home agent injects the mobile networks, which are statically defined or dynamically registered, into its forwarding table. This allows routing protocols configured on the home agent to redistribute these mobile routes.

Routing

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

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

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

Security for Mobile Networks

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

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

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

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

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

Cisco Mobile Networks Redundancy

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

HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic will immediately and transparently recover from failures. An HSRP group comprises two or more routers that share an IP address and a MAC (Layer 2) address and act as a single virtual router. For example, your Mobile IP topology can include one or more standby home agents that the rest of the topology views as a single virtual home agent.

You must define certain HSRP group attributes on the interfaces of the mobile routers so that Mobile IP can implement the redundancy. The mobile routers are aware of the HSRP states and assume the active or standby role as needed. For more information on mobile router redundancy, see the Enabling Mobile Router Redundancy, on page 14 task later in this document. For more information on home agent redundancy, which is a Cisco proprietary feature that runs on top of HSRP, refer to the "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide* , Release 12.2.

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

Benefits

Mobility Solution at the Network Layer

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

Always-On Connection to the Internet

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

Versatile

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

Dynamic Mobile Networks

The dynamic network enables dynamic registration of mobile networks, which results in minimal configuration on the home agent making administration and set up easier. When configured for dynamic registration, the

mobile router tells the home agent which networks are configured in each registration request. The home agent dynamically adds these networks to the forwarding table and there is no need to statically define the networks on the home agent.

Preferred Path

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

Standards-Based Solution

Mobile IP complies with official protocol standards of the Internet.

Mobile IP MIB Support

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

Related Features and Technologies

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

Related Documents

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

Supported Platforms

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

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

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

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

http://tools.cisco.com/ITDIT/MIBS/servlet/inde x

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

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

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

http://www.cisco.com/register

RFCs

- RFC 2003, *IP Encapsulation within IP*
- RFC 2005, *Applicability Statement for IP Mobility Support*
- RFC 2006, *The Definitions of Managed Objects for IP Mobility Support*
- RFC 3024, *Reverse Tunneling for Mobile IP, revised*
- RFC 3344, *IP Mobility Support for IPv4*

Prerequisites

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

Configuration Tasks

Enabling Home Agent Services

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

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

SUMMARY STEPS

1. Router(config)# **router mobile**
2. Router(config-router)# **exit**
3. Router(config)# **ip mobile home-agent**[**address** *ip-address*][**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]
4. Router(config)# **ip mobile virtual-network** *net mask*[**address** *address*]
5. Router(config-router)# **router** *protocol*
6. Router(config)# **redistribute mobile**[**metric** *metric-value*] [**metric-type** *type-value*]
7. Router(config-router)# **exit**
8. Router(config)# **ip mobile host** *lower* [*upper*] {**interface** *name*| **virtual-network** *net mask*} [**lifetime** *number*]
9. Router(config)# **ip mobile mobile-networks** *lower* [*upper*]
10. Router(mobile-networks)# **description** *string*
11. Router(mobile-networks)# **network** *net mask*
12. Router(mobile-networks)# **register**
13. Router(mobile-networks)# **exit**
14. Router(config)# **ip mobile secure host** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.
Step 3	Router(config)# **ip mobile home-agent**[**address** *ip-address*][**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]	Enables home agent service.

	Command or Action	Purpose
	Example:	
Step 4	Router(config)# **ip mobile virtual-network** *net mask*[**address** *address*]	Defines a virtual network. Specifies that the home network is a virtual network, which means that the mobile router is not physically attached to the home agent. Adds the network to the home agent's forwarding table so that routing protocols can redistribute the subnet. If not using virtual networks, go to step 8.
Step 5	Router(config-router)# **router** *protocol*	Configures a routing protocol.
Step 6	Router(config)# **redistribute mobile**[**metric** *metric-value*] [**metric-type** *type-value*]	Enables redistribution of a virtual network into routing protocols.
Step 7	Router(config-router)# **exit**	Returns to global configuration mode.
Step 8	Router(config)# **ip mobile host** *lower* [*upper*] {**interface** *name*| **virtual-network** *net mask*} [**lifetime** *number*]	Configures the mobile router as a mobile host. The IP address is in the home network. The **interface** *name* option configures a physical connection from the home agent to the mobile router.
Step 9	Router(config)# **ip mobile mobile-networks** *lower* [*upper*]	Configures mobile networks for the mobile host and enters mobile networks configuration mode. The *upper* range can be used only with dynamically registered networks and allows you to configure multiple mobile routers at once. The range must match the range configured in the **ip mobile host** command.
Step 10	Router(mobile-networks)# **description** *string*	(Optional) Adds a description to a mobile router configuration.
Step 11	Router(mobile-networks)# **network** *net mask*	(Optional) Configures a network that is attached to the mobile router as a mobile network. Use this command to statically configure networks.
Step 12	Router(mobile-networks)# **register**	(Optional) Dynamically registers the mobile networks with the home agent. The home agent learns about the mobile networks through this registration process. When the mobile router registers its mobile networks on the home agent, the home agent looks up the mobile network configuration and verifies that the **register** command is configured before adding forwarding entries to the mobile networks. If the **register** command is not configured, the home agent will reject an attempt by the mobile router to dynamically register its mobile networks.
Step 13	Router(mobile-networks)# **exit**	Exits mobile networks configuration mode.
Step 14	Router(config)# **ip mobile secure host** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string*	Sets up mobile host security associations. This is the security association the mobile router uses when sending in a registration

	Command or Action	Purpose
		request. The SPI and key between the home agent and mobile router are known. The address is the home IP address of the mobile router.

Enabling Foreign Agent Services

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

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

SUMMARY STEPS

1. Router(config)# **router mobile**
2. Router(config-router)# **exit**
3. Router(config)# **ip mobile foreign-agent care-of** *interface*
4. Router(config)# **interface** *type number*
5. Router(config-if)# **ip address** *ip-address mask*
6. Router(config-if)# **ip irdp**
7. Router(config-if)# **ip irdp maxadvertinterval** *seconds*
8. Router(config-if)# **ip irdp minadvertinterval** *seconds*
9. Router(config-if)# **ip irdp holdtime** *seconds*
10. Router(config-if)# **ip mobile foreign-service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.
Step 3	Router(config)# **ip mobile foreign-agent care-of** *interface*	Enables foreign agent services when at least one care-of address is configured. This is the foreign network termination point of the tunnel between the foreign agent and home agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.
Step 4	Router(config)# **interface** *type number*	Configures an interface and enters interface configuration mode.
Step 5	Router(config-if)# **ip address** *ip-address mask*	Sets a primary IP address of the interface.
Step 6	Router(config-if)# **ip irdp**	Enables IRDP processing on an interface.

	Command or Action	Purpose
Step 7	Router(config-if)# **ip irdp maxadvertinterval** *seconds*	(Optional) Specifies maximum interval in seconds between advertisements.
Step 8	Router(config-if)# **ip irdp minadvertinterval** *seconds*	(Optional) Specifies minimum interval in seconds between advertisements.
Step 9	Router(config-if)# **ip irdp holdtime** *seconds* **Example:**	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the **maxadvertinterval**period.
Step 10	Router(config-if)# **ip mobile foreign-service**	Enables foreign agent service on an interface. This will also append Mobile IP information such as care-of address, lifetime, and service flags to the advertisement.

Enabling Mobile Router Services

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

SUMMARY STEPS

1. Router(config)# **router mobile**
2. Router(config-router)# **exit**
3. Router(config)# **ip mobile router**
4. Router(mobile-router)# **address** *address mask*
5. Router(mobile-router)# **home-agent** *ip-address*
6. Router(mobile-router)# **mobile-network** *interface*
7. Router(mobile-router)# **register** {**extend expire** *seconds* **retry** *number* **interval** *seconds*| **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}
8. Router(mobile-router)# **reverse-tunnel**
9. Router(mobile-router)# **exit**
10. Router(config)# **ip mobile secure home-agent** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*
11. Router(config)# **interface** *type number*
12. Router(config-if)# **ip address** *ip-address mask*
13. Router(config-if)# **ip mobile router-service** {**hold-down** *seconds* | **roam** [**priority** *value*] | **solicit** [**interval** *seconds*] [**retransmit initial** *min* **maximum** *seconds* **retry** *number*]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router mobile**	Enables Mobile IP on the router.
Step 2	Router(config-router)# **exit**	Returns to global configuration mode.
Step 3	Router(config)# **ip mobile router**	Enables the mobile router and enters mobile router configuration mode.
Step 4	Router(mobile-router)# **address** *address mask*	Sets the home IP address and network mask of the mobile router.
Step 5	Router(mobile-router)# **home-agent** *ip-address*	Specifies the home agent that the mobile router uses during registration.
Step 6	Router(mobile-router)# **mobile-network** *interface*	(Optional) Specifies the mobile router interface that is connected to the dynamic mobile network. There can be more than one mobile network configured on a mobile router. The mobile router's registrations will contain these mobile networks.
Step 7	Router(mobile-router)# **register** {**extend expire** *seconds* **retry** *number* **interval** *seconds*| **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}	(Optional) Controls the registration parameters of the mobile router.
Step 8	Router(mobile-router)# **reverse-tunnel**	(Optional) Enables the reverse tunnel function.
Step 9	Router(mobile-router)# **exit**	Exits mobile router configuration mode.
Step 10	Router(config)# **ip mobile secure home-agent** *address* {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string*	Sets up home agent security associations. The SPI and key between the mobile router and home agent are known. The address is the home IP address of the home agent.
Step 11	Router(config)# **interface** *type number*	Configures an interface and enters interface configuration mode.
Step 12	Router(config-if)# **ip address** *ip-address mask*	Sets a primary IP address of the interface.
Step 13	Router(config-if)# **ip mobile router-service** {**hold-down** *seconds* | **roam** [**priority** *value*] | **solicit** [**interval** *seconds*] [**retransmit initial** *min* **maximum** *seconds* **retry** *number*]}	Enables mobile router service, such as roaming, on an interface.

Enabling Mobile Router Redundancy

To enable mobile router redundancy, use the following commands beginning in interface configuration mode. You need not configure HSRP on both the mobile router's roaming interface and the interface attached to the physical mobile networks. If one of the interfaces is configured with HSRP, and the **standby track** command

is configured on the other interface, the redundancy mechanism will work. See the Cisco Mobile Network Redundancy Example, on page 21 section for a configuration example.

SUMMARY STEPS

1. Router(config-if)# **standby**[*group-number*] **ip**[*ip-address*[**secondary**]]
2. Router(config-if)# **standby priority** *priority*
3. Router(config-if)# **standby preempt**
4. Router(config-if)# **standby name** *group-name*
5. Router(config-if)# **standby**[*group-number*] **track** *interface-type interface-number*[*interface-priority*]
6. Router(config-if)# **exit**
7. Router(config)# **ip mobile router**
8. Router(mobile-router)# **redundancy group** *name*

DETAILED STEPS

	Command or Action	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 router.
Step 8	Router(mobile-router)# **redundancy group** *name*	Configures fault tolerance for the mobile router. The *name* argument must match the name specified in the **standby name** *group-name* command.

Verifying Home Agent Configuration

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

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

Verifying Foreign Agent Configuration

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

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

Verifying Mobile Router Configuration

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

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

Verifying Mobile Router Redundancy

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

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

Troubleshooting Tips

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

Monitoring and Maintaining the Mobile Router

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

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

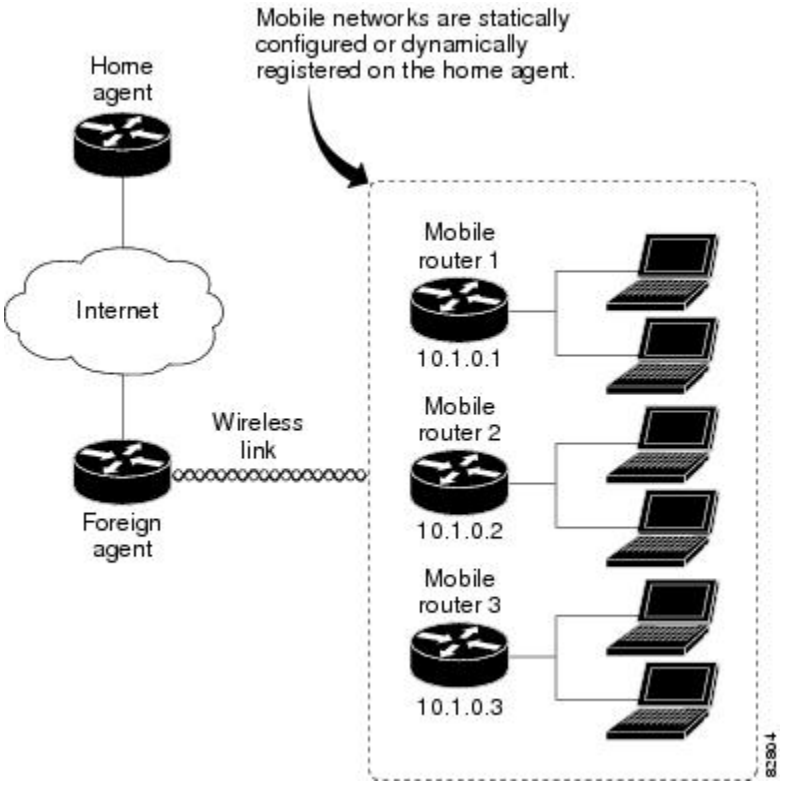
Configuration Examples

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

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

See the figure below for an example topology.

Figure 3: Topology Showing Home Agent Supporting Three Mobile Routers



Home Agent Example

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

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

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

Foreign Agent Example

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

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

Mobile Router Example

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

Mobile Router 1

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

Mobile Router 2

```
interface loopback0
! MR home address
 ip address 10.1.0.2 255.255.255.255
!
interface serial 0
! MR roaming interface
```

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

Mobile Router 3

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

Cisco Mobile Network Redundancy Example

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

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

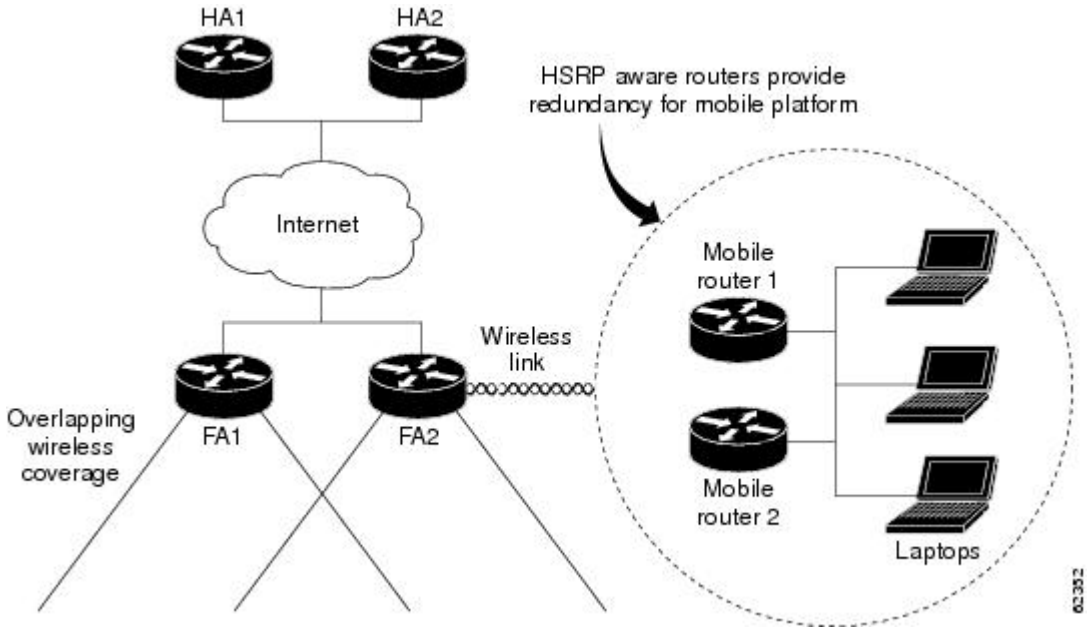
The mobile networks also are defined on the home agent so that the home agent knows to inject these networks into the routing table when the mobile router is registered.

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

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

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

Figure 4: Topology Showing Cisco Mobile Networks Redundancy



Home Agent 1 (HA1) Configuration

```
interface Ethernet1/1
 ip address 100.100.100.3 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 duplex half
 standby ip 100.100.100.1
 standby priority 100
 standby preempt delay sync 60
!HSRP group name
 standby name HA_HSRP2
!
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent
! Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network address 100.100.100.1
```

```
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
ip mobile mobile-networks 70.70.70.70
 description san jose jet
! Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.2 spi 300 key hex 123456781234967812345678123456789
```

Home Agent 2 (HA2) Configuration

```
interface Ethernet1/1
 ip address 100.100.100.2 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 standby ip 100.100.100.1
 standby priority 95
 standby preempt delay sync 60
! HSRP group name
 standby name HA_HSRP2
!
router mobile
!
router rip
 version 2
 redistribute mobile
 network 100.0.0.0
 default-metric 1
!
ip classless
ip mobile home-agent
!Maps to HSRP group name
ip mobile home-agent redundancy HA_HSRP2 virtual-network address 100.100.100.1
ip mobile virtual-network 70.70.70.0 255.255.255.0
ip mobile host 70.70.70.70 virtual-network 70.70.70.0 255.255.255.0
ip mobile mobile-networks 70.70.70.70
 description san jose jet
!Mobile Networks
 network 20.20.20.0 255.255.255.0
 network 10.10.10.0 255.255.255.0
ip mobile secure host 70.70.70.70 spi 100 key hex 12345678123456781234567812345678
ip mobile secure home-agent 100.100.100.1 spi 300 key hex 123459781234567812345678123456789
```

Foreign Agent 1 (FA1) Configuration

```
interface Ethernet0
 ip address 171.69.68.2 255.255.255.0
 media-type 10BaseT
!
interface Ethernet1
 ip address 80.80.80.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip irdp holdtime 30
 ip mobile foreign-service
 media-type 10BaseT
!
router mobile
!
router rip
 version 2
 network 80.0.0.0
 network 100.0.0.0
!
ip classless
```

```
no ip http server
ip mobile foreign-agent care-of Ethernet1
```

Foreign Agent 2 (FA2) Configuration

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

Mobile Router 1 Configuration

```
interface Ethernet5/2
! MR roaming interface
 ip address 70.70.70.4 255.255.255.0
 ip mobile router-service roam
! Configure redundancy for mobile router using HSRP
 standby ip 70.70.70.70
 standby priority 105

standby preempt
 standby name MR_HSRP2
 standby track Ethernet5/4
!
interface Ethernet5/4
! Interface to Mobile Network
 ip address 20.20.20.2 255.255.255.0
!
router mobile
!
router rip
 version 2
 passive-interface Ethernet5/2
 network 20.0.0.0
 network 70.0.0.0
!
ip classless
no ip http server
ip mobile secure home-agent 100.100.100.100 spi 100 key hex 12345678123456781234567812345678

ip mobile router
! Maps to HSRP group name
 redundancy group MR_HSRP2
! Using roaming interface hot address as MR address
 address 70.70.70.70 255.255.255.0
 home-agent 100.100.100.1
```

Mobile Router 2 Configuration

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

ip mobile router
! Maps to HSRP group name
 redundancy group MR_HSRP2
! Using roaming interface hot address as MR address
 address 70.70.70.70 255.255.255.0
 home-agent 100.100.100.1
```

Command Reference

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

- **address (mobile router)**
- **clear ip mobile router agent**
- **clear ip mobile router registration**
- **clear ip mobile router traffic**
- **debug ip mobile**
- **debug ip mobile router**
- **description (mobile networks)**
- **home-agent**
- **ip mobile mobile-networks**
- **ip mobile router**

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

Glossary

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

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

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

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

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

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

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

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

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

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

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

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

mobility agent --A home agent or a foreign agent.

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

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

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

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

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

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

node --A host or router.

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

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

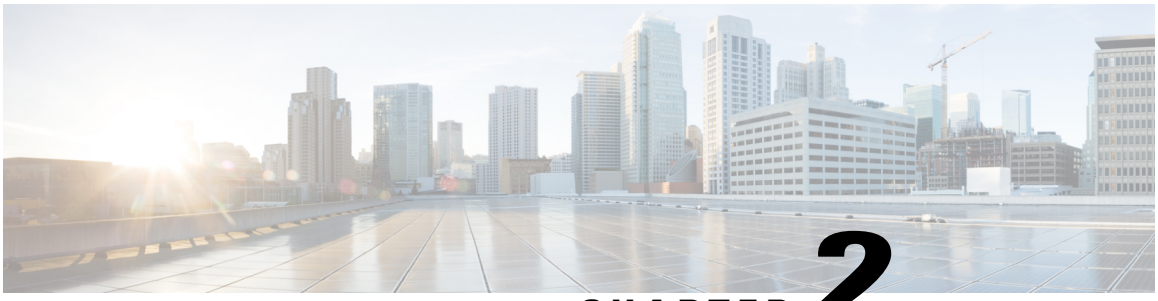
SPI --security parameter index. The index identifying a security context between a pair of nodes. On the home agent, the SPI identifies which shared secret to use to compute the md5 hash value.

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

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

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

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



CHAPTER 2

Cisco Mobile Networks Asymmetric Link

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

Feature Specifications for the Cisco Mobile Networks: Asymmetric Link

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

Finding Feature Information

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

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

Restrictions for Cisco Mobile Networks Asymmetric Link

This feature can be used only on serial interfaces.

Information About Cisco Mobile Networks Asymmetric Link

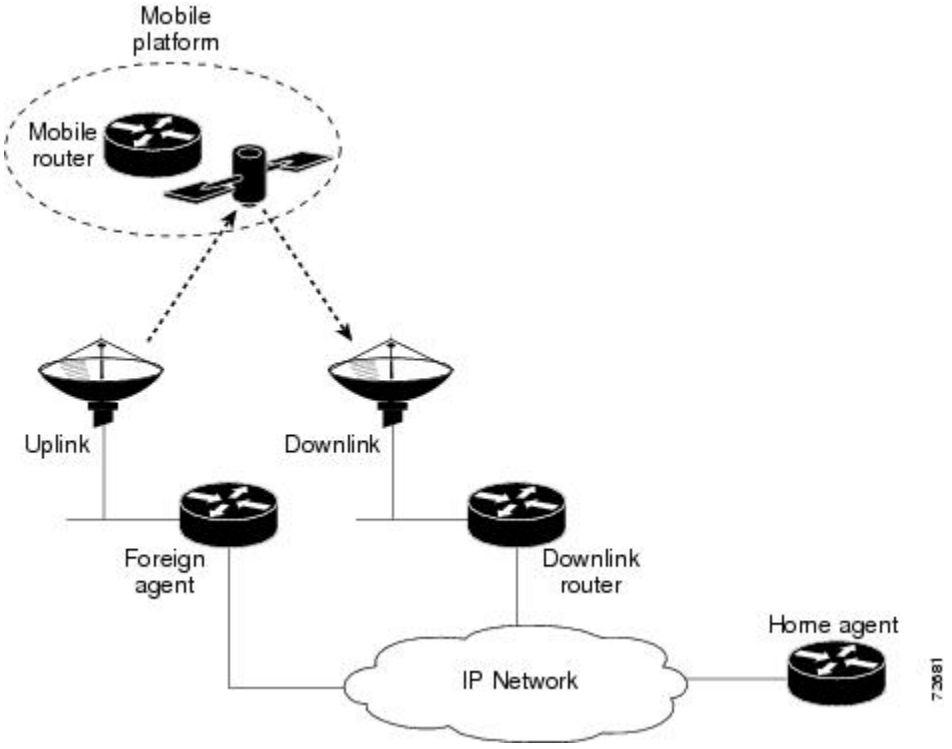
Unidirectional Routing in Cisco Mobile Networks

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

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

The figure below shows how packets are routed within the mobile network using unidirectional routing.

Figure 5: Unidirectional Routing in an Asymmetric Communications Environment



How to Configure Mobile Networks in an Asymmetric Link Environment

Enabling Mobile Router Services for Unidirectional Interfaces

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 1`	Configures an interface type and enters interface configuration mode.
Step 4	**transmit-interface** *type number*	Assigns a transmit interface to a receive-only interface.

	Command or Action	Purpose
	Example: `Router(config-if)# transmit-interface serial 2`	• This is the uplink (receive-only) interface. • In the example, this command specifies interface serial 2, connected to the downlink router, to be the transmit-only interface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.6.2 255.255.255.0`	Sets a primary IP address for an interface. • This is the IP address of a roaming interface.
Step 6	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables the mobile router to specify on which configured interface it will discover foreign agents.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface serial 2`	Configures an interface type and enters interface configuration mode. • This is the downlink (transmit-only) interface that was specified in Step 4.
Step 9	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.7.2 255.255.255.0`	Sets a primary IP address for an interface. • This is the IP address of a roaming interface.
Step 10	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables the mobile router to specify on which configured interface it will discover foreign agents.

Troubleshooting Tips

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

Enabling Foreign Agent Services for Unidirectional Interfaces

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 1`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.2 255.255.255.0`	Sets a primary IP address of the interface.
Step 5	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables IRDP processing on an interface.
Step 6	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 4`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 7	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 3`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 8	**ip irdp holdtime** *seconds* **Example:** `Router(config-if)# ip irdp holdtime 10`	(Optional) Length of time in seconds that advertisements are held valid. • Default is three times the **maxadvertinterval**period.
Step 9	**ip mobile foreign-service** **Example:** `Router(config-if)# ip mobile foreign-service`	Enables foreign agent service on an interface. • This command also appends Mobile IP information such as care-of address, lifetime, and service flags to the advertisement.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.

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

Enabling Home Agent Services

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

Verifying Cisco Mobile Networks Asymmetric Link Configuration

SUMMARY STEPS

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

DETAILED STEPS

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

What to Do Next

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

```
Router# show ip mobile globals
IP Mobility global information:
Home Agent is not enabled
Foreign Agent
   Pending registrations expire after 15 secs
   Care-of addresses advertised
    Serial4/0 (11.0.0.2) - up, interface-only, transmit-only
```

Configuration Examples for Cisco Mobile Networks Asymmetric Link

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

Mobile Router Example

The following example shows the mobile router configuration:

```
!
interface Loopback1
 ip address 20.0.4.1 255.255.255.0
```

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

Foreign Agent Example

The following example shows the foreign agent configuration:

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

Additional References

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

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the*Cisco IOS IP Configuration Guide,*Release 12.2.
Mobile IP commands	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* , Release 12.2.
Cisco Mobile Networks commands	"Cisco Mobile Networks" feature document, Release 12.2(4)T.

Standards

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

MIBs

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

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

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

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

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

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

http://www.cisco.com/register

RFCs

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

Technical Assistance

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

Command Reference

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

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

Glossary

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

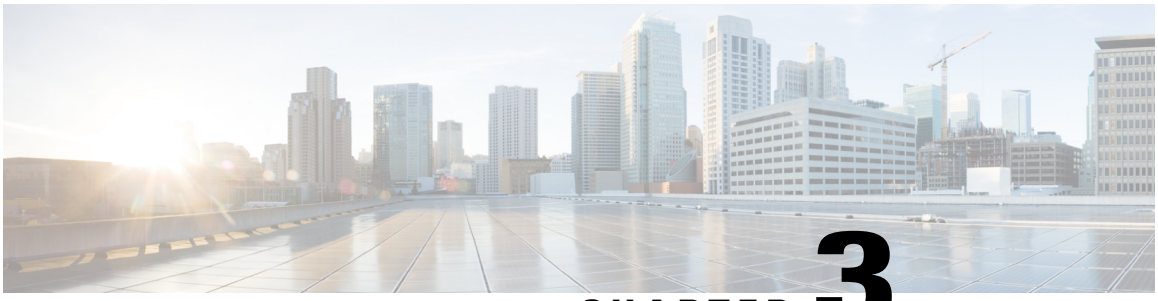
foreign agent --A router on the visited network of a foreign network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers packets to the mobile node or mobile router that were tunneled by the home agent of the mobile node. For packets sent by a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

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

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

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

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



CHAPTER 3

Cisco Mobile Networks Static Collocated Care-of Address

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

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

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

Finding Feature Information

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

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

Prerequisites for Cisco Mobile Networks Static CCoA

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

Restrictions for Cisco Mobile Networks Static CCoA

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

Information About the Cisco Mobile Networks Static CCoA

Care-of Addresses

If a mobile node or mobile router determines that it is connected to a foreign network, it acquires a care-of address. This care-of address is the exit-point of the tunnel towards the mobile node. The care-of address is included in the Mobile IP registration request and is used by the home agent to forward packets to the mobile node in its current location. Two types of care-of addresses exist:

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

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

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

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

Benefits of Cisco Mobile Networks Static CCoA

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

Feature Design of Cisco Mobile Networks Static CCoA

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

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

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

How to Configure Cisco Mobile Networks Static CCoA

Enabling Static CCoA Processing on a Mobile Router Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip-address 168.71.6.23 255.255.255.0`	Sets a primary IP address for an interface. • This is the static CCoA.
Step 5	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 6	**ip mobile router-service collocated** [**gateway** *ip-address*] **Example:** `Router(config-if)# ip mobile router-service collocated gateway 168.71.6.1`	Enables static CCoA processing on a mobile router. • The gateway IP address is the next hop IP address for the mobile router to forward packets. The gateway IP address is required only on Ethernet interfaces, and must be on the same logical subnet as the primary interface address specified in Step 4.
Step 7	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You only need to use this command when a different retry interval is desired.

Troubleshooting Tips

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

Verifying the Static CCoA Configuration

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for Cisco Mobile Networks Static CCoA

Mobile Networks with Static CCoA Example

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

```
interface loopback 0
! MR home address
 ip address 10.1.0.1 255.255.255.255
!
!Static CCoA
interface FastEthernet0/0
 ip address 172.21.58.23 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 172.21.58.1
 ip mobile router-service collocated registration retry 3
!
router mobile
!
ip mobile router
 address 10.1.0.1 255.255.255.255
 home-agent 1.1.1.1
ip mobile secure home-agent 1.1.1.1 spi 100 key hex 12345678123456781234567812345678
```

Additional References

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

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the *Cisco IOS IP Configuration Guide,* Release 12.2
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2
Mobile IP commands related to Cisco Mobile Networks	"Cisco Mobile Networks" feature document, Release 12.2(4)T and 12.2(13)T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

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

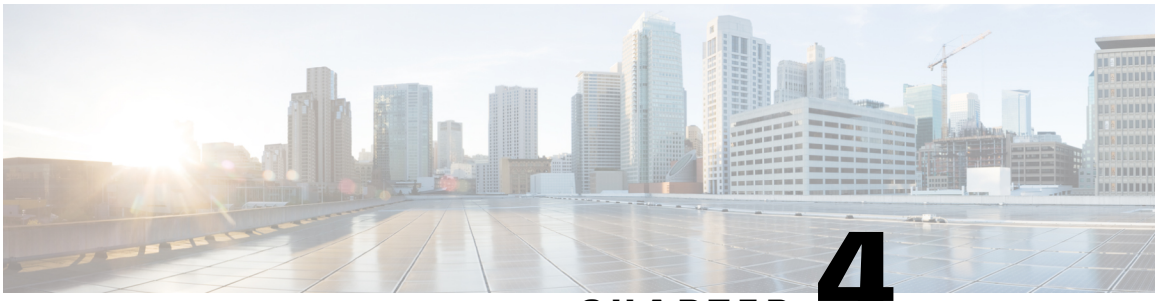
Glossary

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

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

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

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



CHAPTER 4

Cisco Mobile Networks Priority HA Assignment

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

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

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

Finding Feature Information

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

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

Information About Cisco Mobile Networks Priority HA Assignment

Feature Design of Cisco Mobile Networks Priority HA Assignment

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

Best HA Selection Process

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

Benefits of Cisco Mobile Networks Priority HA Assignment

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

How to Configure Cisco Mobile Networks Priority HA Assignment

Configuring Care-of Address Access Lists on an HA

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

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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile home-agent care-of-access** *access-list* **Example:** `Router(config)# ip mobile home-agent care-of-access HA1-FA1`	Controls which care-of addresses in registration requests are permitted by the home agent. • By default, all care-of addresses are permitted. The access list can be a string or number from 1 to 99.
Step 4	**ip access-list standard** *access-list-name* **Example:** `Router(config)# ip access-list standard HA1-FA1`	Defines a standard access list and enters standard named access list configuration mode. • Use this command to configure access lists on each HA that is reachable by the mobile router.
Step 5	**permit** *coa-ip-address* **Example:** `Router(config-std-nacl)# permit 3.3.3.2`	Sets conditions for an access list. • The *coa-ip-address* can be a foreign agent care-of address or a collocated care-of address. This command informs the HA which care-of addresses can be accepted in a registration request.
Step 6	**permit** *mr-home-address* **Example:** `Router(config-std-nacl)# permit 5.5.5.3`	Sets conditions for an access list. • The *mr-home-address* is the home address for the mobile router. See the Troubleshooting Tips, on page 54 section below for an explanation as to why it is important to include the mobile router home address.
Step 7	**exit** **Example:** `Router(config-std-nacl)# exit`	Exits to global configuration mode.

	Command or Action	Purpose
Step 8	**router** *protocol* **Example:** `Router(config)# router ospf`	Configures a routing protocol.
Step 9	**redistribute mobile subnets** **Example:** `Router(config-router)# redistribute mobile subnets`	Enables redistribution of a virtual network into routing protocols.
Step 10	**distribute-list** *access-list* **out** **Example:** `Router(config-router)# distribute-list 1 out`	(Optional) Suppresses networks from being advertised in updates. • This command configured on each HA will prevent the advertisement of the virtual network for the mobile routers. See the Configuring Care-of Address Access Lists on an HA and Troubleshooting Tips, on page 54 sections for more information about using this command.
Step 11	**exit** **Example:** `Router(config-router)# exit`	Exits to global configuration mode.
Step 12	**access-list** *access-list-number* **deny** *source* **Example:** `Router(config)# access-list 1 deny 5.5.5.0`	Defines a standard IP access list. • Denies access if the conditions are matched. • In this example, the *source* value is the the virtual network configured on the HA. The **distribute-list** command in Step 10 prevents the advertisement of this virtual network.
Step 13	**access-list** *access-list-number* **permit any** **Example:** `Router(config)# access-list 1 permit any`	Defines a standard IP access list. • Permits access if the conditions are matched.
Step 14	Repeat Steps 3 through 7 for each HA configured on the mobile router. Repeat Steps 8 through 13 for each HA if virtual networks are configured.	--

Troubleshooting Tips

Care-of Address List Operation

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

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

Virtual Network Advertisements

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

Configuring HA Priorities on the Mobile Router

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.

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

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

Examples

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

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

```
Router# show ip mobile router
Mobile Router
  Enabled 01/01/02 10:01:34
  Last redundancy state transition NEVER
Configuration:
  Home Address 5.5.5.3 Mask 255.255.255.0
  Home Agent 200.200.200.1 Priority 102 (best) (current)
        100.100.100.1 Priority 101
  Registration lifetime 90 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
```

```
  Extend Expire 120, Retry 3, Interval 10
Monitor:
  Status -Registered-
  Active foreign agent 3.3.3.2, Care-of 3.3.3.2
  On interface Ethernet5/3
```

Configuration Examples for Cisco Mobile Networks Priority HA Assignment

HA Priority Configuration Example

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

Home Agent1

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

Home Agent 2

```
interface Loopback0
 ip address 200.200.200.1 255.255.255.255
!
interface Ethernet0
 ip address 1.1.1.1 255.255.255.0
!
```

```
router mobile
!
router ospf 100
 redistribute mobile subnets
 network 1.0.0.0 0.255.255.255 area 0
 network 200.200.200.0 0.255.255.255 area 0
! Suppresses virtual network to be advertised in update
 distribute-list 1 out
!
ip mobile home-agent care-of-access HA2-FA2
ip mobile virtual-network 5.5.5.0 255.255.255.0
ip mobile host 5.5.5.3 virtual-network 5.5.5.0 255.255.255.0 lifetime 90
ip mobile mobile-networks 5.5.5.3
 description Jet
 network 6.6.6.0 255.255.255.0
ip mobile secure host 5.5.5.3 spi 200 key hex 12345678123456781234567812345678 algorithm
md5 mode prefix-suffix
!
ip access-list standard HA2-FA2
! FA COA
 permit 3.3.3.2
! MR home address
 permit 5.5.5.3
!
access-list 1 deny 5.5.5.0 0.0.0.255
access-list 1 permit any
```

Mobile Router

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

Additional References

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

Related Documents

Related Topic	Document Title
Mobile IP configuration tasks	"Configuring Mobile IP" chapter in the *Cisco IOS IP Configuration Guide,* Release 12.2
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	"Mobile IP Commands" chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 T
Mobile IP commands related to Cisco mobile networks	*Cisco Mobile Networks* feature document, Release 12.2(4)T and 12.2(13)T
Access list commands	*"IP Services Commands"* chapter in the*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Glossary

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

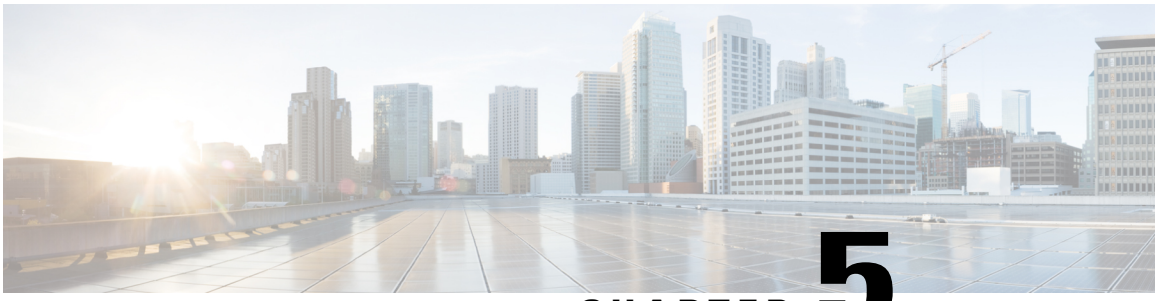
home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding .

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

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

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

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



CHAPTER 5

Cisco Mobile Networks Tunnel Templates for Multicast

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

Feature Specifications for Cisco Mobile Networks-Tunnel Templates for Multicast

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

Finding Feature Information

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

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

Prerequisites for Cisco Mobile Networks Tunnel Templates for Multicast

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

Restrictions for Cisco Mobile Networks Tunnel Templates for Multicast

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

How to Configure Tunnel Templates for Multicast

Applying the Tunnel Template on the Home Agent

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**interface tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 100`	Designates a tunnel interface and enters interface configuration mode. • This is the tunnel template that will be applied to the mobile networks.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on the tunnel interface in sparse mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 8	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.

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

Examples

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

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel1:
    src 1.1.1.1, dest 20.20.0.1
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1460 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Tunnel0
    HA created, fast switching enabled, ICMP unreachable enabled
    27 packets input, 2919 bytes, 0 drops
    24 packets output, 2568 bytes
Running template configuration for this tunnel:
ip pim sparse-dense-mode
Tunnel0:
    src 1.1.1.1, dest 30.30.10.2
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Ethernet1/3
    HA created, fast switching enabled, ICMP unreachable enabled
    0 packets input, 0 bytes, 0 drops
    24 packets output, 3048 bytes
```

Applying the Tunnel Template on the Mobile Router

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**interface tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 100`	Designates a tunnel interface and enters interface configuration mode. • This is the tunnel template that will be applied to the mobile networks.
Step 5	**ip pim sparse-mode**	Enables PIM on the tunnel interface in sparse mode.

	Command or Action	Purpose
	Example: `Router(config-if)# ip pim sparse-mode`	
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 8	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 9	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 10	**template tunnel** *interface-number* **Example:** `Router(mobile-router)# template tunnel 100`	Designates the tunnel template to apply during registration. • The *interface number*argument is set to the tunnel template defined in Step 4.
Step 11	**end** **Example:** `Router(mobile-router)# end`	Exits to privileged EXEC mode.
Step 12	**show ip mobile tunnel** **Example:** `Router# show ip mobile tunnel`	Displays active tunnels. • Use this command to verify the configuration.

Examples

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

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

Configuration Examples for Tunnel Templates for Multicast

Tunnel Templates for Multicast Example

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

Home Agent Configuration

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

Mobile Router Configuration

```
!
ip multicast-routing
!
interface Loopback0
 ip address 11.1.0.1 255.255.255.255
 ip pim sparse-mode
!
!
! Tunnel template to be applied to mobile networks
interface tunnel 100
 no ip address
 ip pim sparse-mode
!
!
interface Ethernet1/1
 ip address 20.0.0.1 255.0.0.0
 ip pim sparse-mode
 ip mobile router-service roam
!
router mobile
ip pim rp-address 7.7.7.7
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781 algorithm
 md5 mode prefix-suffix
ip mobile router
 address 11.2.0.1 255.255.0.0
 home-agent 1.1.1.1
! Select tunnel template to apply during registration
 template tunnel 100
 register extend expire 5 retry 2 interval 15
 register lifetime 10000
 reverse-tunnel
!
```

Additional References

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

Related Documents

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

Related Topic	Document Title
Mobile IP commands related to Cisco Mobile Networks	*Cisco Mobile Networks* feature document, Releases 12.2(4)T and 12.2(13)T.

Standards

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

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

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

Technical Assistance

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

Command Reference

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

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

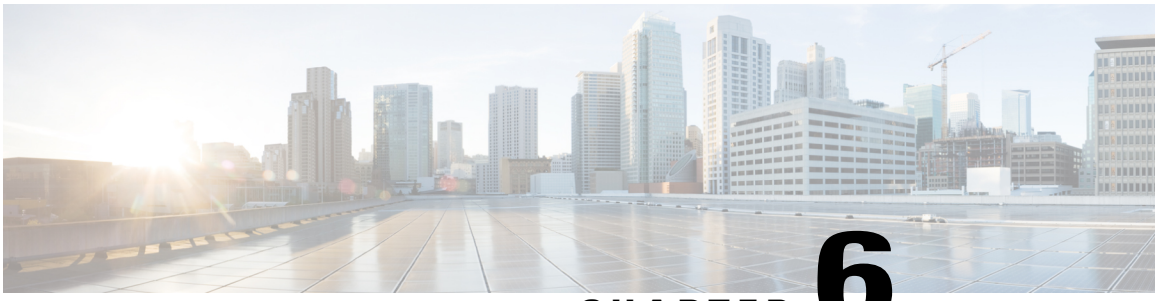
Glossary

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

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

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

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



CHAPTER 6

Mobile Networks Dynamic Collocated Care-of Address

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

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

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

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

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

Finding Feature Information

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

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

Restrictions for Mobile Networks Dynamic CCoA

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

Information About Mobile Networks Dynamic CCoA

Care-of Addresses

If a mobile router determines that it is connected to a foreign network, it acquires a care-of address. This care-of address is the exit point of the tunnel from the home agent toward the mobile router. The care-of address is included in the Mobile IP registration request and is used by the home agent to forward packets to the mobile router in its current location. There are two types of care-of addresses:

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

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

Mobile Networks Dynamic CCoA Feature Design

The Mobile Networks Dynamic CCoA feature is very similar to the static CCoA implementation. Static CCoA uses the address configured on the roaming interface as the CCoA. Dynamic CCoA uses IPCP to obtain a CCoA for the roaming interface. See the http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcolloc.htm Cisco Mobile Networks - Static Collocated Care-of Address feature documentation for more information on the static CCoA implementation.

For both static and dynamic CCoA, the interface can be configured to exclusively use CCoAs for registration or to use a foreign agent CoA if one is available. In the foreign agent case, when an interface first comes up, it will attempt to discover foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile router will register using the advertised CoA. The interface will continue to register using a CoA as long as a foreign agent is heard. When foreign agents are not heard, either because

no advertisements are received or the foreign agent advertisement hold time expires, CCoA processing is enabled and the interface registers its CCoA. The CCoA is the interface's statically configured or dynamically acquired primary IP address. If a foreign agent is heard again, the interface will again register the foreign agent CoA.

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

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

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

Benefits of Mobile Networks Dynamic CCoA

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

How to Configure Mobile Networks Dynamic CCoA

Enabling Dynamic CCoA Processing on a Mobile Router Interface

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 1`	Configures an interface type and enters interface configuration mode. • Dynamic CCoAs can be acquired only on serial interfaces.
Step 4	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is obtained via IPCP address negotiation.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP enacapsulation on a specified serial interface.
Step 6	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 7	**ip mobile router-service collocated** **Example:** `Router(config-if)# ip mobile router-service collocated`	Enables CCoA processing on a mobile router interface. • The interface will first solicit foreign agent advertisements and register with a foreign agent CoA if an advertisement is heard. If no advertisements are received, CCoA registration is attempted.
Step 8	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You need to use this command only when a different retry interval is desired.

Enabling CCoA-Only Processing on a Mobile Router Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	Do one of the following: • **ip address** *ip-address mask*	Sets a primary IP address for an interface. • This is the static CCoA. Static CCoAs can be configured on serial or Ethernet interfaces.

	Command or Action	Purpose

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

Step 5	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 6	**ip mobile router-service collocated ccoa-only** **Example:** `Router(config-if)# ip mobile router-service collocated ccoa-only`	Enables CCoA-only processing on a mobile router interface. • This command can be used on serial interfaces for dynamic or static CCoA processing. • This command disables foreign-agent CoA processing and limits the interface to CCoA processing only. • If you use this command on an interface already registered with a foreign agent CoA, the mobile router will re-register immediately with a CCoA.
Step 7	**ip mobile router-service collocated gateway** *ip-address* **ccoa-only** **Example:** `Router(config-if)# ip mobile router-service collocated gateway 10.21.0.2 ccoa-only`	(Optional) Enables CCoA-only processing on a mobile router interface. • This command can be used only on Ethernet interfaces for static CCoA processing. • The gateway IP address is the next hop IP address for the mobile router to forward packets. The gateway IP address is required only on Ethernet interfaces, and must be on the same logical subnet as the primary interface.

	Command or Action	Purpose
Step 8	**ip mobile router-service collocated registration retry** *seconds* **Example:** `Router(config-if)# ip mobile router-service collocated registration retry 3`	(Optional) Configures the time period that the mobile router waits before sending another registration request after a registration failure. • The default value is 60 seconds. You need to use this command only when a different retry interval is desired.

Verifying the Dynamic CCoA Configuration

Perform this task to verify the dynamic CCoA configuration:

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**show ip mobile router** **Example:** `Mobilerouter# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.
Step 5	**show ip mobile binding** **Example:** `Homeagent# show ip mobile router`	Displays the mobility binding table. • If a CCoA is registered with the home agent, (D) direct-to-mobile node is displayed in the Routing Options field.

Configuration Examples for Mobile Networks Dynamic CCoA

Mobile Networks Dynamic CCoA Example

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

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

Mobile Networks with CCoA-Only Processing Example

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

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

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

```
interface loopback1
```

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

Additional References

The following sections provide additional references related to the Mobile Networks Dynamic CCoA feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility,* Release 12.3 T
Mobile IP commands and configuration tasks related to mobile networks	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks feature document, Release 12.2(4)T and 12.2(13)T
Static CCoA documentation	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcolloc.htm Cisco Mobile Networks - Static Collocated Care-of Address , Release 12.2(15)T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

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

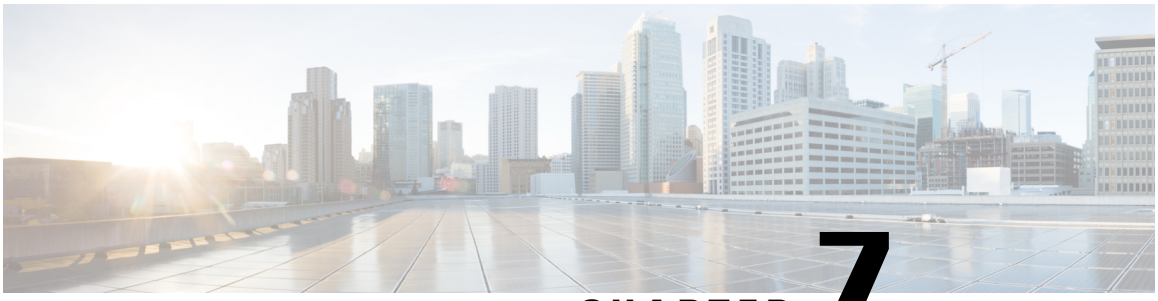
Glossary

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

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

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

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



CHAPTER 7

Mobile Networks Deployment MIB

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

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

Feature History for the Mobile Networks Deployment MIB Feature

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

Finding Feature Information

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

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

Additional References

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

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility,* Release 12.3 T
Mobile IP commands and configuration tasks related to mobile networks	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks, Cisco IOS Release 12.2(4)T and Release 12.2(13)T
Cisco configuration fundamentals and network management commands	*Cisco IOS Configuration Fundamentals and Network Management Command Reference,* Release 12.3 T

Standards

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

MIBs

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

RFCs

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

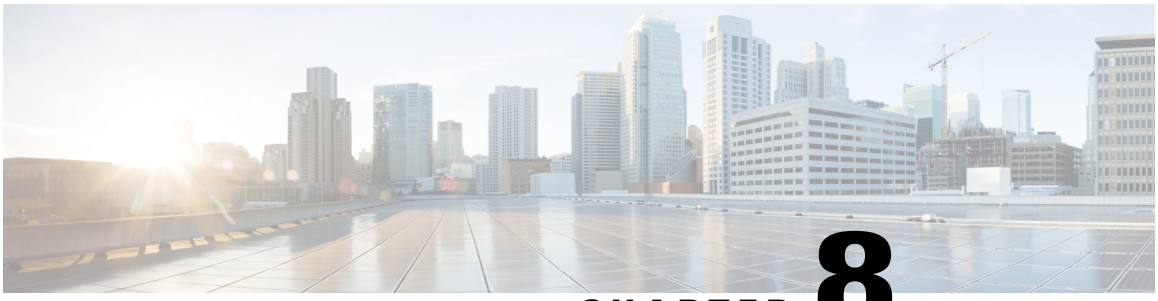
Technical Assistance

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

Command Reference

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

- **debug ip mobile mib**



CHAPTER 8

Mobile IP - Foreign Agent Local Routing to Mobile Networks

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

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

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

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

Finding Feature Information

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

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

Prerequisites for Foreign Agent Local Routing to Mobile Networks

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

Restrictions for Foreign Agent Local Routing to Mobile Networks

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

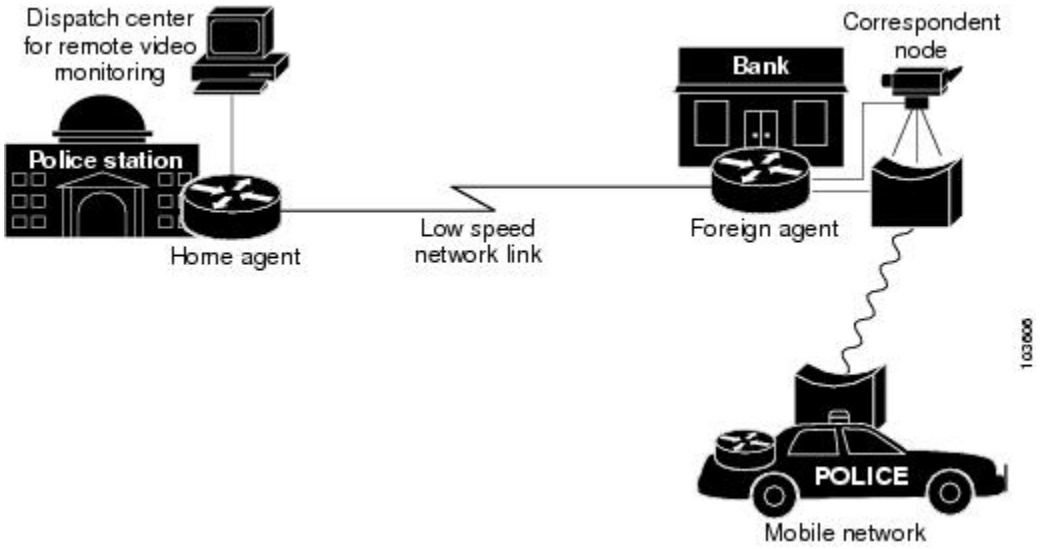
Information About Foreign Agent Local Routing to Mobile Networks

Foreign Agent Local Routing to Mobile Networks Feature Design

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

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

Figure 6: Usage Scenario for the Mobile IP - Foreign Agent Local Routing to Mobile Networks Feature



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

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

Benefits of Foreign Agent Local Routing to Mobile Networks

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

How to Configure Foreign Agent Local Routing to Mobile Networks

Configuring Local Routing to Mobile Networks on the Foreign Agent

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile foreign-agent inject-mobile-networks** [**mobnetacl** *access-list-identifier*] **Example:** `Router(config)# ip mobile foreign-agent inject-mobile-networks mobnetacl mobile-net-list`	Enables direct routing to the mobile networks via the foreign agent.
Step 4	**ip mobile secure** {**aaa-download** | **host** | **visitor** | **home-agent**| **foreign-agent**| **proxy-host**} {*lower-address*[*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*]] [**algorithm** {**md5 mode prefix-suffix**| **hmac-md5**}] **Example:** `Router(config)# ip mobile secure home-agent 10.10.10.1 spi`	Specifies the mobility security associations for the mobile host, visitor, home agent, and foreign agent.

	Command or Action	Purpose
	1400 key hex 12345678123456781234567812345678 algorithm hmac-md5	

Troubleshooting Tips

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

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

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

Configuring an Access List

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

Configuring a Named Access List

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list** {**standard** | **extended**} *access-list-name* **Example:** `Router(config)# ip access-list standard mobile-net-list`	Defines an IP access list by name.
Step 4	[*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `Router(config-std-nacl)# permit any`	Sets conditions to allow a packet to pass a named IP access list.

Configuring a Numbered Access List

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines a standard IP access list.

	Command or Action	Purpose
	Example: `Router(config)# access-list 88 permit any`	

Configuration Examples for Foreign Agent Local Routing to Mobile Networks

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

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

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

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

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

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

Additional References

The following sections provide references related to the Mobile IP - Foreign Agent Local Routing to Mobile Networks feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3 T
Mobile IP commands and configuration tasks related to mobile networks	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks feature document, Release 12.2(4)T and Release 12.2(13)T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

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

Glossary

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

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

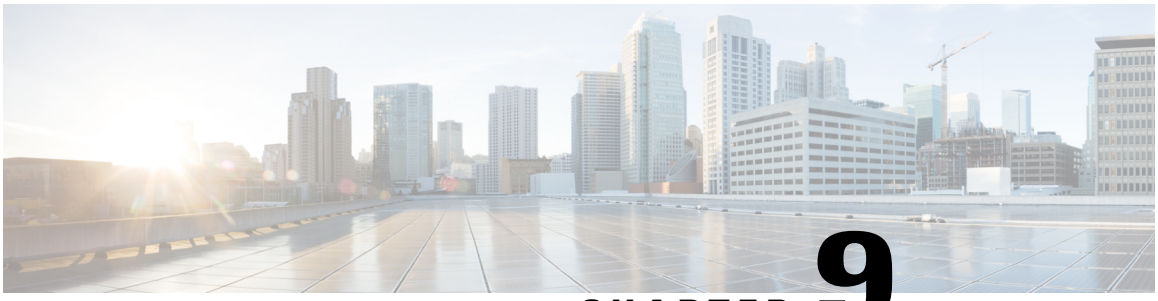
home agent --A router on a home network of the mobile node that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding.

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

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

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

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



CHAPTER 9

Mobile IP - Generic Routing Encapsulation for Cisco Mobile Networks

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

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

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

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

Finding Feature Information

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

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

Prerequisites for GRE for Cisco Mobile Networks

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

Restrictions for GRE for Cisco Mobile Networks

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

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

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

Information About GRE for Cisco Mobile Networks

Generic Routing Encapsulation

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

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

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

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

GRE for Cisco Mobile Networks Feature Design

To understand the components of the Cisco Mobile Networks solution, refer to the http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks feature documentation.

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

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

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

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

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

GRE Keepalive Messages

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

Benefits of GRE for Cisco Mobile Networks

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

How to Configure GRE for Cisco Mobile Networks

Configuring GRE on the Mobile Router

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

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

Configuring GRE Globally on the Mobile Router

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.

	Command or Action	Purpose

Step 4	**tunnel mode gre**
	
	Example:
	`Router(mobile-router)#`
	`tunnel mode gre`
		Sets the global encapsulation mode on all roaming interfaces of a mobile router to GRE.
		
		Note Configuring an encapsulation protocol on an interface overrides the globally configured encapsulation protocol on that interface only. If there is no interface-level configuration, the interface inherits the global configuration.

Step 5	**end** **Example:** `Router(mobile-router)#` **end**	Ends the current configuration session and returns to privileged EXEC mode.
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuring GRE per Interface on the Mobile Router

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 2`	Configures an interface type and enters interface configuration mode.
Step 4	**ip mobile router-service tunnel mode** {**gre** | **ipip**} **Example:** `Router(config-if)# ip mobile router-service tunnel mode gre`	Sets the encapsulation mode for a mobile router interface. • **gre** --Specifies that the mobile router will attempt to register with GRE encapsulation on the interface. • **ipip** --Specifies that IP-in-IP encapsulation will be used on the interface. **Note** Configuring an encapsulation protocol on an interface overrides the globally configured encapsulation protocol on that interface only. If there is no interface-level configuration, the interface inherits the global configuration.
Step 5	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays the pending and accepted registrations of the mobile router.
Step 7	**show ip mobile router interface** **Example:** `Router# show ip mobile router interface`	Displays information about the interface that the mobile router is using for roaming.

Configuring GRE Keepalive Messages

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *interface-number* **Example:** `Router(config)# interface tunnel 121`	Enters interface configuration mode for the specified interface.
Step 4	**keepalive** [**period** [**retries**]] **Example:** `Router(config-if)# keepalive 5 3`	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)#` **exit**	Returns to global configuration mode.
Step 6	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 7	**template tunnel** *interface-number* **Example:** `Router(mobile-router)# template tunnel 121`	Applies a tunnel template to tunnels brought up at the mobile router.

Configuration Examples for GRE for Cisco Mobile Networks

Configuring GRE for Cisco Mobile Networks Globally Example

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

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

Configuring GRE for Cisco Mobile Networks on an Interface Example

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

```
interface FastEthernet0/0
 ip address 10.52.52.2 255.255.255.0
 ip mobile router-service roam
```

```
 ip mobile router-service tunnel mode gre
!
interface tunnel 121
 keepalive 5 3
!
ip mobile router
 template tunnel 121
```

Verifying GRE for Cisco Mobile Networks Examples

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

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

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

```
Router# show ip mobile router
Mobile Router
    Enabled 01/11/00 06:59:19
    Last redundancy state transition NEVER
Configuration:
    Home Address 10.80.80.1 Mask 255.255.255.0
    Home Agent 10.40.40.1 Priority 100 (best) (current)
    Registration lifetime 65534 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 20, Retry 10, Interval 1
    Request GRE tunnel
    Mobile Networks:Ethernet1/3 (172.16.143.0/255.255.255.0)
                    FastEthernet0/0 (172.16.153.0/255.255.255.0)
Monitor:
    Status -Registered-
    Active foreign agent 10.52.52.1, Care-of 10.52.52.1
    On interface FastEthernet0/0
    Tunnel0 mode GRE/IP
```

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

```
Router# show ip mobile router interface
FastEthernet0/0:
    Priority 110, Bandwidth 100000, Address 10.52.52.2
    Periodic solicitation disabled, Interval 600 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Current 2000, Remaining 0 msec, Count 2
    Hold down 0 sec
    Routing disallowed
```

```
Collocated CoA disabled
Request GRE tunnel
```

Additional References

The following sections provide references related to the GRE for Mobile Networks feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3 T
Mobile IP commands and configuration tasks related to mobile networks	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks feature document, Release 12.2(4)T and 12.2(13)T
Additional information about GRE keepalives	*Generic Routing Encapsulation (GRE) Tunnel Keepalive* feature document, Release 12.2(8)T
Information on configuring quality of service (QoS) with GRE	Quality of Service Options on GRE Tunnel Interfaces

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

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

Glossary

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

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

care-of address --The termination point of the tunnel to a mobile node or mobile router. This can be a collocated care-of address, by which the mobile node or mobile router acquires a local address and detunnels

its own packets, or a foreign agent care-of address, by which a foreign agent detunnels packets and forwards them to the mobile node or mobile router.

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

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

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

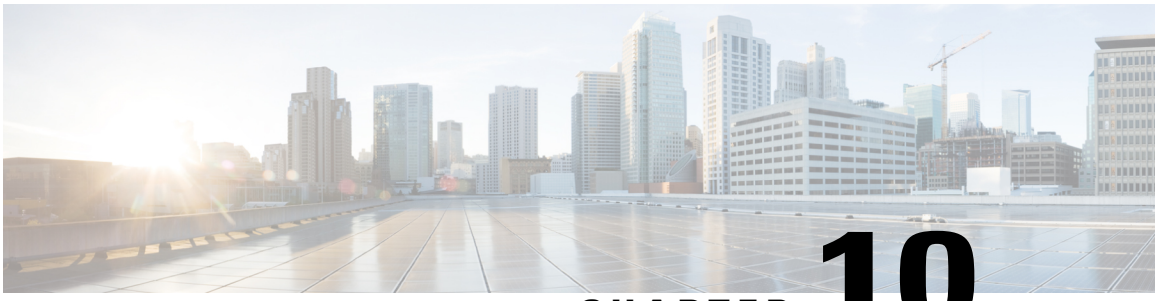
mobile network --A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

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

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

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

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



CHAPTER 10

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

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

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

Finding Feature Information

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

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

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

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

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

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

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

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

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

This document uses the terms "mobile node" and "mobile router." Most of the conceptual information in this document applies to both a mobile node and a mobile router. The term "mobile router" also applies to the Cisco 3200 Mobile Access Router. Refer to the Glossary, on page 119 section for definitions of these terms.

NAT Traversal Support Overview

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

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

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

UDP-tunneled packets that have been sent by a mobile node use the same ports as the registration request message. The source port may vary between new registration requests but remains the same for all tunneled data and reregistrations. The destination port is always 434. UDP- tunneled packets that are sent by a home agent use the same ports, but in reverse.

When the registration request packet traverses a NAT-enabled router, the home agent detects the traversal by comparing the source IP address of the packet with the CoA inside the request. If the two addresses differ, the home agent detects that a NAT gateway exists in the middle. If the home agent is configured to accept NAT traversal, it accepts the registration request and enables the use of UDP tunneling, and the data traffic passes through the NAT gateway. Thereafter, any traffic from the home agent to the mobile node is sent through the UDP tunnel. If there is a foreign agent, the foreign agent must also be configured for NAT traversal in order for UDP tunneling to work. See the Mobile IP Support for NAT Traversal on the Mobile Router Feature Design, on page 111 section for information about the scenario in which the mobile router chooses to register with the home agent using a private CCoA.

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

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

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

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

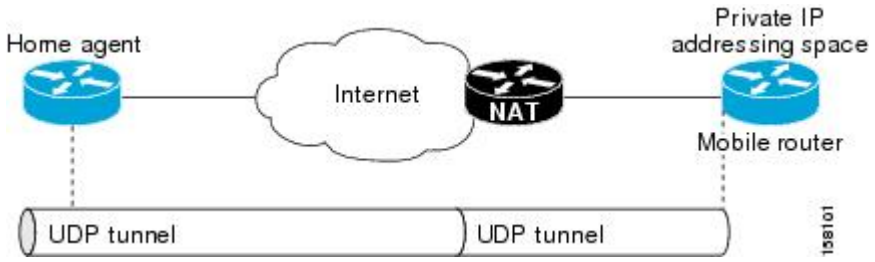
Mobile IP Support for NAT Traversal on the Mobile Router Feature Design

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

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

tunnel and will restart the registration process. The figure below shows the UDP tunnel that was set up between the home agent and the mobile router.

Figure 7: Topology Showing the UDP Tunnel Between the Home Agent and the Mobile Router



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

Configuring the Mobile Router for NAT Traversal Support

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip mobile router-service collocated registration nat traversal [keepalive** *seconds* **] [force]** **Example:** `Router(config-if)# ip mobile router-service collocated registration nat traversal keepalive 45 force`	Enables NAT traversal support for the mobile router. The keywords and arguments are as follows: • **keepalive** *seconds* --(Optional) Configures the keepalive interval, in seconds, that the mobile router will use when the home agent does not offer a specific value and just returns zero. The range is from is 0 to 65535. The default is 110. **Note** Setting the *keepalive-time* argument to zero disables the keepalive timer. The mobile router does not use the keepalive interval unless the home agent sends back a zero in the registration reply. • **force** --(Optional) Allows the mobile router to force the home agent to allocate a NAT UDP tunnel without performing detection presence of NAT along the HA-MR path. **Note** If you configure the mobile router to force the home agent to allocate a UDP tunnel but do not configure the home agent to force UDP tunneling, the home agent will reject the forced UDP tunneling request. The decision of whether to force UDP tunneling is controlled by the home agent.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring the Home Agent for NAT Traversal Support

SUMMARY STEPS

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

DETAILED STEPS

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

Step 3	**ip mobile home-agent nat traversal** [**keepalive** *seconds*] [**forced** {**accept** | **reject**}]
	
	Example:
	`Router(config)# ip mobile home-agent nat`
	`traversal keepalive 45 forced accept`
		Enables NAT traversal support for the home agent. The keywords and argument are as follows:
		• **keepalive** *seconds* --(Optional) Time, in seconds, between keepalive messages that are sent between UDP endpoints to refresh NAT translation timers. The range is 0 to 65535. The default is 110.
		• **forced** --(Optional) Enables the home agent to accept or reject forced UDP tunneling from the mobile node regardless of the NAT-detection outcome.
		• **accept**--Accepts UDP tunneling.
		• **reject**--Rejects UDP tunneling. This is the default behavior.

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

Verifying Mobile Router NAT Traversal Support

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]
3. **show ip mobile globals**
4. **show ip mobile tunnel** [*interface*]
5. **show ip mobile router interface**
6. **show ip mobile router registration**
7. **show ip mobile router**

DETAILED STEPS

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

	Command or Action	Purpose
Step 6	**show ip mobile router registration** **Example:** `Router# show ip mobile router registration`	Displays pending and/or accepted registrations of the mobile router.
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

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

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

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

Home Agent Configuration

```
interface Loopback1
 ip address 198.168.2.1. 255.255.255.255
!
router mobile
!
! The following command sets the UDP keepalive interval to 60 seconds and enables the HA !
 to accept forced UDP tunneling registration requests.
!
ip mobile home-agent nat traversal keepalive 60 forced accept
ip mobile home-agent
ip mobile virtual-network 10.99.100.0 255.255.255.0
ip mobile host 10.99.100.1 10.99.100.100 virtual-network 10.99.100.0 255.255.255.0
ip mobile mobile-networks 10.99.100.2
 description MAR-3200
 register
!
ip mobile secure host 10.99.100.1 10.99.100.100 spi 100 key hex
12345678123456781234567812345678 algorithm md5 mode prefix-suffix
```

Mobile Router Configuration

```
interface Loopback1
! Description MR's home address.
ip address 10.99.100.2 255.255.255.255
!
interface FastEthernet0/0
 description Wi-Fi Link
 ip address 10.5.3.32 255.255.255.0
```

```
! The following command sets the UDP keepalive interval to 60 seconds and enables the !
mobile router to request UDP tunneling.
 ip mobile router-service collocated registration nat traversal keepalive 60 force
 ip mobile router-service roam priority 120
!
ip mobile router
 address 10.99.100.2 255.255.255.0
 collocated single-tunnel
 home-agent 10.1.1.1 priority 110
 mobile-network Vlan210
 reverse-tunnel
```

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

- **ip mobile router-service collocated registration nat traversal**

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

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

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

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

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

Glossary

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

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

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

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

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

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

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

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

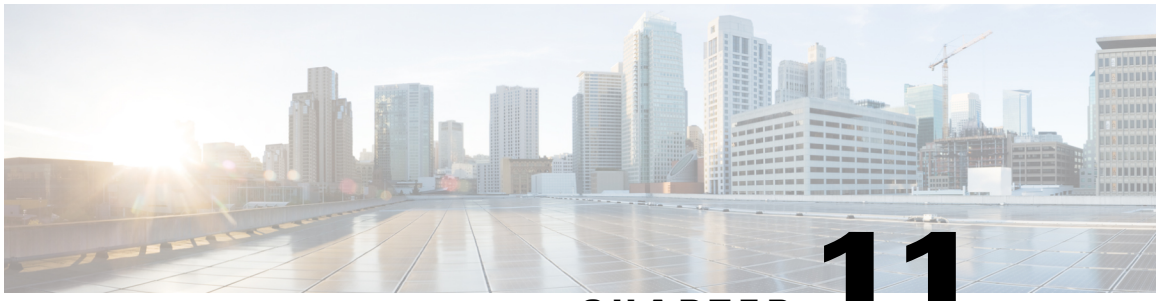
mobile node --A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming that link-layer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

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

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

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

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



CHAPTER 11

Mobile IP Policy and Application-Based Routing for MR Multipath

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

Finding Feature Information

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

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

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

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

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

Policy-based application routing has the following restrictions:

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

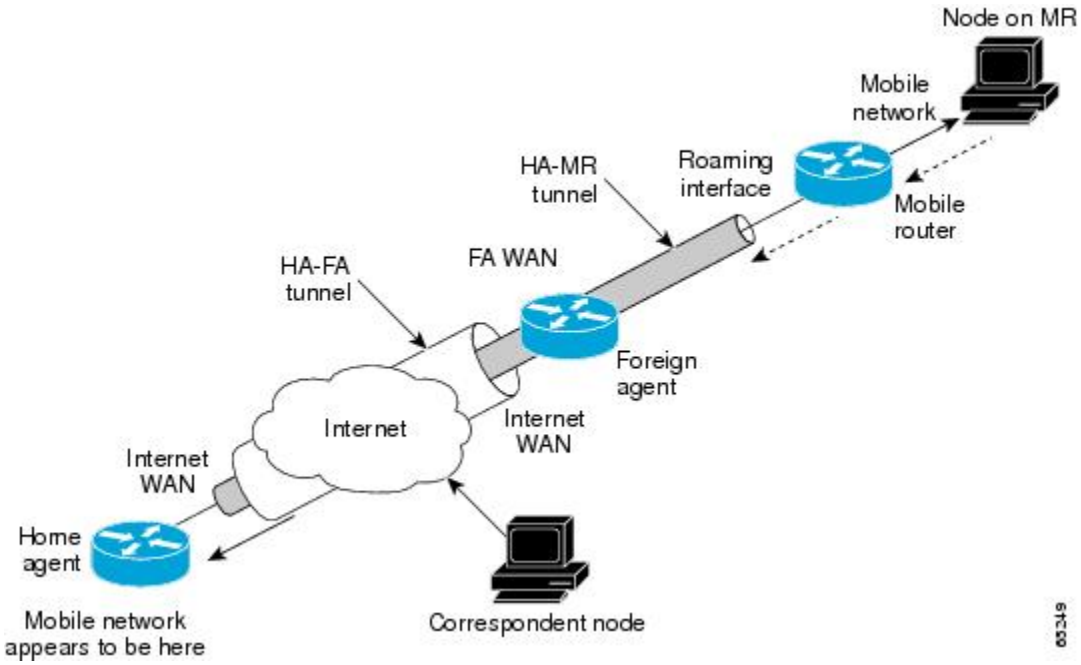
Information About Mobile IP Policy and Application-Based Routing for MR Multipath

Mobile Router Multipath Support Feature Design

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

de-encapsulation. The MR then sent the original packets to the IP devices on the mobile networks. See the figure below for an illustration of routing within a mobile network using a single tunnel.

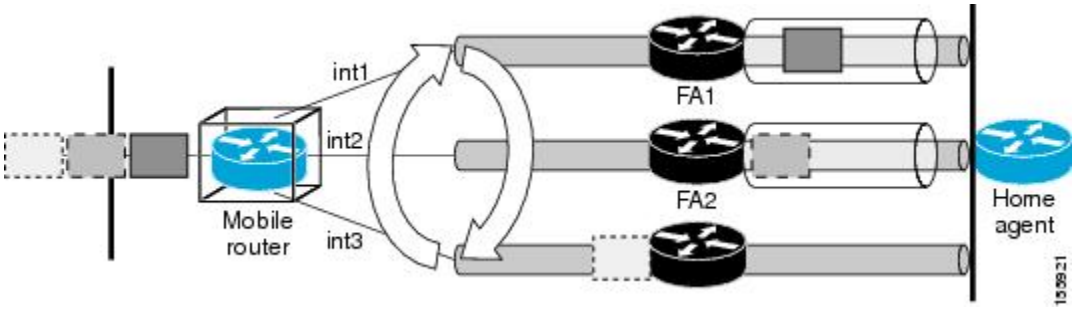
Figure 8: Routing Within the Mobile Network Using a Single Tunnel



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

See the figure below for an illustration of the mobile router registering through multiple interfaces.

Figure 9: Mobile Router Registering Through Multiple Interfaces to the Home Agent



Upon successful registration, the HA maintains multiple care-of addresses, mobility bindings, tunnels, and routes to the same MR. Multiple bindings are not the same as simultaneous bindings. With multiple bindings,

the traffic is not replicated on all tunnels but rather load-balanced across them, which means that the packets are sent through only one path.

Mobile Router Multipath Load-Balancing Behavior

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

Policy-based application routing allows you to control the roaming interface that is used by an application to route its traffic to the other end of a Mobile IP tunnel. This provides flexibility to control how the applications are routed over different mobile wireless networks based on a defined policy. The applications are policy-routed based on the roaming interface type. See the Routing Based on Policies and Selecting Roaming Interfaces, on page 127 for more information on policy-based application routing.

Setting Priority Levels and MR Registration

You can configure policy-based application routing and the MR roaming interfaces. You should set the priority levels when you enable the roaming interface. The MR registers on multiple roaming interfaces based on the roaming interface configuration. The MR registers only through the highest priority interface. If there is more than one interface with the same highest priority, then both interfaces are used by the MR during registration. If all highest priority interfaces are unavailable, then the MR switches to the next available highest priority interface. The interfaces have link-type labels configured on them. See Registering the MR Based on the Roaming Priority Example, on page 139 for an example.

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

Benefits of Mobile Router Multipath Support

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

How to Configure Mobile Router Multipath Support

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

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

This section contains the following tasks:

Configuring the Mobile Router for Multipath Support

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

Before You Begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **exit**
6. **router mobile**
7. **exit**
8. **ip mobile router**
9. **address** *address mask*
10. **home-agent** *ip-address*
11. **mobile-network** *interface-type interface number*
12. **multi-path** [**metric** {**bandwidth** | **hopcount**}]
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface loopback0`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	Sets a primary IP address of the interface. • This is the home address of the mobile router.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 6	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router and enters router configuration mode.
Step 7	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 8	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 9	**address** *address mask* **Example:** `Router(mobile-router)# address 209.165.200.225 255.255.255.224`	Sets the home IP address and network mask of the mobile router.
Step 10	**home-agent** *ip-address* **Example:** `Router(mobile-router)# home-agent 192.0.2.19`	Specifies the home agent that the mobile router uses during registration.

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

What to Do Next

Routing Based on Policies and Selecting Roaming Interfaces

This section contains the following topics:

Before You Begin

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

Example:

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/2`	Configures an interface and enters interface configuration mode.
Step 4	**ip mobile router-service roam priority** *priority-level* **Example:** `Router(config-if)# ip mobile router-service roam priority 101`	Enables the roaming interface and sets the priority level. The roaming interface priority defaults to 100 if priority is not specified while configuring the **ip mobile router-service roam** command.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Enabling the Roaming Interfaces

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/2`	Configures an interface and enters interface configuration mode.
Step 4	**ip mobile router-service roam priority** *priority-level* **Example:** `Router(config-if)# ip mobile router-service roam priority 101`	Enables the roaming interface and sets the priority level. The roaming interface priority defaults to 100 if priority is not specified while configuring the **ip mobile router-service roam**command.
Step 5	**ip mobile router-service link-type** *label* **Example:** `Router(config-if)# ip mobile router-service link-type 802.11g`	Enables a link-type roaming interface.
Step 6	**end** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.

Defining the Traffic Policies

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

Identifying the Application Traffic

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list extended** *access-list name* **Example:** `Router(config)# ip access-list extended WEB`	Configures an extended named ACL.
Step 4	**permit udp any any eq** *port* **Example:** `Router(config-ext-nacl)# permit udp any any eq 8080`	Identifies the application traffic to be policy routed. These are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route-maps.
Step 5	**end** **Example:** `Router(config-ext-nacl)# end`	Returns to privileged EXEC mode.

Selecting the Routing Path

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

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service roam priority** *priority level*
5. **ip mobile router-service link-type** *label*
6. **exit**
7. **ip access-list extended** *access-list-name*
8. **permit udp any any eq** *port*
9. **exit**
10. **ip mobile mobile-map** *map name*
11. **match access-list** *acl*
12. **set link-type** *label*
13. **set interface** *interface-type number*
14. **ip mobile router**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

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

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

Configuring the Home Agent for Multipath Support

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router and enters router configuration mode.
Step 4	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.
Step 5	**ip mobile home-agent multi-path** [**metric** {**bandwidth**	**hopcount**}] **Example:** `Router(config)# ip mobile home-agent multi-path`	Enables the home agent to process registration requests with multiple path support for all mobile routers. • Bandwidth is the default metric.

	Command or Action	Purpose
Step 6	**ip mobile virtual-network** *net mask* [**address** *address*] **Example:** `Router(config)# ip mobile virtual-network 209.165.200.225 255.255.255.224`	Defines a virtual network. Specifies that the home network is a virtual network, which means that the mobile router is not physically attached to the home agent. Adds the network to the home agent's forwarding table so that routing protocols can redistribute the subnet.
Step 7	**ip mobile host** *lower* [*upper*] {**interface**name | **virtual-network** *net mask*} **Example:** `Router(config)# ip mobile host 209.165.200.219 255.255.255.224 virtual-network 209.165.200.225 255.255.255.224`	Configures the mobile router as a mobile host. The IP address is in the home network. • The **interface** *name* option configures a physical connection from the home agent to the mobile router.
Step 8	**ip mobile mobile-networks** *lower* [*upper*] **Example:** `Router(config)# ip mobile mobile-networks 209.165.200.219 209.165.200.225`	Configures mobile networks for the mobile host and enters mobile networks configuration mode. The *upper* range can be used only with dynamically registered networks and allows you to configure multiple mobile routers at once. • The range must be within the range configured in the **ip mobile host** command.
Step 9	**register** **Example:** `Router(mobile-networks)# register`	Dynamically registers the mobile networks with the home agent.
Step 10	**multi-path** [**metric** {**bandwidth** | **hopcount**}] **Example:** `Router(mobile-networks)# multi-path`	Configures the global default setting and enables the home agent to process requests with multiple path support for a specific mobile router. Bandwidth is the default metric.
Step 11	**exit** **Example:** `Router(mobile-networks)# no multi-path`	Returns to privileged EXEC mode.

What to Do Next

After you configure the HA you can define the traffic policies. This enables you to identify a particular traffic from the mobile networks and then select the tunnel for routing the traffic. This provides flexibility to control

how the applications are routed over different mobile wireless networks based on a policy. See the "Defining the Traffic Policies, on page 129" for more information on how to define the traffic policies.

Clearing the Mobility Binding on the Home Agent

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

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

>

SUMMARY STEPS

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

DETAILED STEPS

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

Verifying Mobile Router Multipath Support

Perform this task to verify MR multipath support.

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]
3. **show ip mobile global**
4. **show ip mobile mobile-networks**
5. **show ip mobile tunnel** [*interface*]
6. **show ip route**
7. **show ip mobile router**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip mobile binding** [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**] **Example:** `Router# show ip mobile binding`	Displays the mobility binding on the home agent.
Step 3	**show ip mobile global** **Example:** `Router# show ip mobile global`	Displays global information for mobile agents.
Step 4	**show ip mobile mobile-networks** **Example:** `Router# show ip mobile mobile-networks`	Displays a list of mobile networks that are associated with the mobile router.
Step 5	**show ip mobile tunnel** [*interface*] **Example:** `Router# show ip mobile tunnel`	Displays active tunnels.
Step 6	**show ip route** **Example:** `Router# show ip route`	Displays the current state of the routing table.

	Command or Action	Purpose
Step 7	**show ip mobile router** **Example:** `Router# show ip mobile router`	Displays configuration information and monitoring statistics about the mobile router.

Configuration Examples for Mobile Router Multipath Support

Multipath Support on the Mobile Router Example

The following example shows how to configure multipath support on the mobile router:

```
interface Loopback0
! MR home address
 ip address 209.165.200.225 255.255.255.224
interface Tunnel101
 keep 5 3
interface Ethernet1/0
! MR roaming interface
 ip address 209.165.200.239 255.255.255.224
 ip mobile router-service roam
interface Ethernet2/0
! MR roaming interface
 ip address 209.165.200.246 255.255.255.224
 ip mobile router-service roam
interface Ethernet3/0
 ip address 209.165.200.247 255.255.255.224
router mobile
ip mobile router
 address 209.165.200.251 255.255.255.224
 home-agent 192.0.2.12
 mobile-network Ethernet3/0
 tunnel mode gre
 multi-path
 template Tunnel101
ip mobile secure home-agent 192.0.2.16 spi 101 key hex 12345678901234567890123456789012
```

Multipath Support on the Home Agent Example

The following example shows how to configure multipath support on the home agent:

```
interface Ethernet 0/0
 ip address 209.165.200.251 255.255.255.224
!
router mobile
 exit
 ip mobile home-agent multi-path
 ip mobile virtual-network 209.165.200.252 255.255.255.224
 ip mobile host 192.0.2.10 192.0.2.15 virtual-network 209.165.200.254 255.255.255.224
 ip mobile secure host 192.0.2.20 192.0.2.25 spi 101 key hex  12345678901234567890123456789012
ip mobile mobile-networks 192.0.2.40 192.0.2.44
 register
```

```
ip mobile mobile-networks 192.0.2.57
 register
 no multi-path
```

Registering the MR Based on the Roaming Priority Example

The following example shows how roaming priority levels are selected during MR registration:

Consider the following four interfaces:

```
interface Fastethernet 1/0
  ip mobile router-service roam priority 200
  ip mobile router-service link-type 802.11g
interface Fastethernet 1/1
  ip mobile router-service roam priority 200
  ip mobile router-service link-type 802.11g
interface Fastethernet 2/0
  ip mobile router-service roam priority 100
  ip mobile router-service link-type 802.11g
interface Fastethernet 2/1
  ip mobile router-service roam priority 100
  ip mobile router-service link-type 802.11g
Fast Ethernet interfaces 1/0 and 1/1 have priority 200. Fast Ethernet interfaces 2/0 and
2/1 have priority 100. When you try enabling these four interfaces, the MR registers on
both the Fast Ethernet interfaces 1/0 and 1/1 because they have the highest roaming priority.
 But when the interfaces Fastethernet 1/0 and 1/1 are not available, the MR registers on
Fastethernet 2/0 and 2/1, the next available highest priority group.
```

Using mobile-map Mobile Policy Templates Example

The following example shows to use the mobile-map mobile policy templates on the MR and the HA to select the routing path.

```
ip mobile mobile-map MPATH_1 10
 match access-list WEB
 set link-type 802.11g UMTS
 set interface null0
```

Generating Dynamic Route Maps in an HA Example

The following example shows how the dynamic route maps are generated in an HA:

```
Router# show route-map dynamic
route-map MIP-10/24/06-04:18:15.243-1-MP-HA, permit, sequence 0, identifier 53856096
  Match clauses:
    ip address (access-lists): VOICE-to-192.0.2.0/24
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
Router# show ip access-lists dynamic
Extended IP access list VOICE-to-192.0.2.0/24
    10 permit icmp any 209.165.200.225 255.255.255.224 tos max-reliability
```

Additional References

The following sections provide references related to the Mobile IP-- Policy and Application-Based Routing for MR Multipath Support feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Mobility Command Reference*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

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

- **clear ip mobile binding**
- **debug ip mobile dyn-pbr**
- **ip mobile home-agent multi-path**
- **ip mobile router-service link-type**
- **ip mobile router-service roam**
- **multi-path (mobile networks)**
- **multi-path (mobile router)**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile mobile-networks**
- **show ip mobile router interface**
- **show ip mobile router registration**
- **show ip mobile tunnel**

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

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

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

Table 2: Feature Information for Mobile IP-- Policy and Application-Based Routing for MR Multipath

Feature Name	Releases	Feature Information
Mobile IP--Mobile Router Multipath Support	12.4(9)T	This Mobile IP--Mobile Router Multipath Support feature provides support for multiple paths, and thus multiple wireless technologies, between the mobile router and the home agent and allows user traffic to be load-balanced over all available interfaces.
Mobile IP-- Policy and Application-Based Routing for MR Multipath	12.4(24)T	This feature provides support for mobile router multipath registration based on roaming interface priority; application routing based on link or path type; and multiple registrations based on roaming interface priority. The following commands were introduced: **ip mobile router-service link-type**, **ip mobile router-service roam**. The following commands were modified: **show ip mobile binding, show ip mobile router interface, show ip mobile router registration, show ip mobile tunnel**

Glossary

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

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

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

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

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

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

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

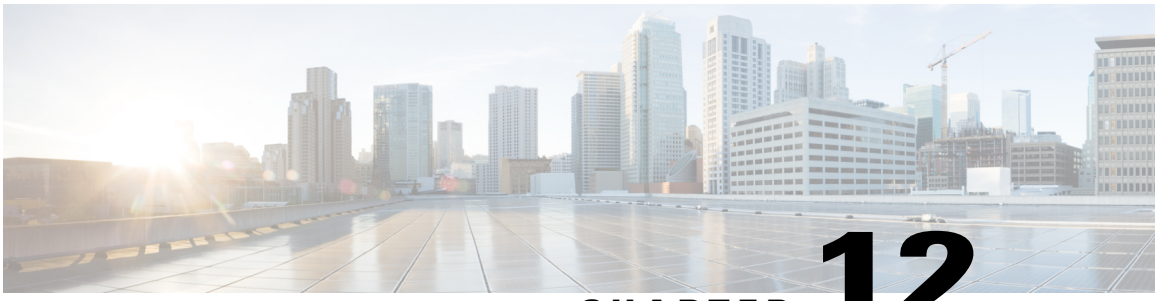
mobile router --A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile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

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

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

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

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



CHAPTER 12

Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing

The Mobile Router DHCP Support for Dynamic Collocated Care-of Address (DCCoA) and Foreign Agent (FA) Processing feature adds support for mobile router roaming on Ethernet interfaces that acquire an IP address dynamically via the Dynamic Host Configuration Protocol (DHCP). The interface can register using this acquired IP address as a DCCoA or register using a CoA acquired from a foreign agent. This behavior is true for all platforms that support Mobile IP beginning with Cisco IOS Release 12.3(14)T.

This feature adds support for FA processing of advertisements and registrations on DHCP roaming interfaces.

A Simple Network Management Protocol (SNMP) signaling capability is also added to support this feature on the Cisco 3200 Series Mobile Access Router with a Wireless Mobile Interface Card (WMIC). The WMIC uses SNMP trap messages to signal the mobile router that the Layer 2 wireless local-area network (WLAN) is either up or down.

Feature History for the Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing Feature

Release	Modification
12.3(14)T	This feature was introduced.

Finding Feature Information

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

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

Prerequisites for Mobile Router DHCP Support for DCCoA and FA Processing

There are no prerequisites for DHCP support. However, if a Cisco 3200 Series Mobile Access Router is using a WMIC, the WMIC should be configured for SNMP traps. The 802.11 Layer 2 transitions (associations and disassociations) that take place on the WMIC are signaled to the mobile router via SNMP. Specifically, the Interface MIB linkUp and linkDown traps are sent to the mobile router Ethernet or VLAN interface.

See the Configuration Guide for the Cisco 3200 Series Mobile Access Router for more information on how to configure SNMP traps on the Cisco 3200 Series router.

Restrictions for Mobile Router DHCP Support for DCCoA and FA Processing

The Mobile IP process will only process SNMP signals from a WMIC. The SNMP signaling functionality for DCCoA is supported on the Cisco 3200 Series Mobile Access Router.

The linkDown and linkUp trap events will not trigger mobile router redundancy.

Information About Mobile Router DHCP Support for DCCoA and FA Processing

Care-of Addresses

If a mobile router determines that it is connected to a foreign network, it acquires a CoA. This CoA is the exit point of the tunnel from the home agent toward the mobile router. The CoA is included in the mobile router's registration request and is used by the home agent to forward packets to the mobile router in its current location. There are two types of CoAs:

- CoA acquired from a foreign agent
- Collocated care-of address (CCoA)

A foreign agent CoA is an IP address on a foreign agent that is advertised on the foreign network being visited by a mobile router. A foreign agent CoA can be shared by other mobile routers.

A CCoA is an IP address assigned to the interface of the mobile router itself. A CCoA represents the current position of the mobile router on the foreign network and can be used by only one mobile router at a time. A CCoA can be static or dynamic. A static CCoA is a fixed IP address configured on an interface. A dynamic CCoA is an IP address dynamically acquired via DHCP on an Ethernet interface or Point-to-Point Protocol (PPP)/IP Control Protocol (IPCP) on a point-to-point serial interface.

An interface enabled for both foreign agent CoA and CCoA registration will always register a foreign agent CoA instead of a CCoA if a foreign agent CoA is available.

Mobile Router DHCP Support

This feature introduces DCCoA and foreign agent CoA support when IP addresses are obtained via DHCP on a roaming interface. Prior to the introduction of this feature, the mobile router could only support foreign agent CoA registration, static CCoA registration, and DCCoA registration through PPP/IPCP.

For both static and dynamic CCoA, the interface can be configured to exclusively use the CCoA for registration or to use a foreign agent CoA if one is available. An interface enabled for both foreign agent CoA and CCoA registration will always register a foreign agent CoA instead of a CCoA if a foreign agent CoA is available.

In the foreign agent case, when an interface first comes up, it will attempt to discover foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile router will register using the advertised CoA. The interface will continue to register using a CoA as long as a foreign agent is heard. When foreign agents are not heard, CCoA processing is enabled and the interface registers its CCoA. The CCoA is the interface's statically configured or dynamically acquired primary IP address. If a foreign agent is heard again, the interface will again register using the foreign agent CoA.

In previous releases of CCoA support, the CCoA registration would begin only after a number of solicits were sent or no advertisements were heard. For faster roaming, this delay is now eliminated. Now the interface registers a foreign agent CoA if an agent advertisement is heard or it registers a CCoA if an address is acquired, depending on which event occurs first. In the case where the interface registers a CCoA first, a subsequent receipt of an agent advertisement will then cause the interface to register with the foreign agent.

To support CCoA on Ethernet interfaces, a default gateway address is required. This gateway address is used as the default gateway for CCoA registration and as a default route after the interface is registered. For static CCoA on an Ethernet interface, a default gateway address must be provided through the roaming interface CCoA configuration. See the Cisco IOS Release 12.2(15)T Mobile Networks Static Collocated Care-of Address feature documentation for configuration details.

When an interface is configured for DCCoA via DHCP, a configured gateway address is not required and the option to configure a gateway address is not offered through the command line interface (CLI). For DHCP interfaces, DCCoA registration uses the DHCP default router address and, once the interface is registered, the address is also used for the mobile router default route and gateway.

Mobile Router Support for SNMP Traps

On a Cisco 3200 Series Mobile Access Router with a WMIC, SNMP traps allow the roaming interface to determine when the connected WLAN link status changes. Without this signaling, a CCoA-registered interface would not be aware of link status changes. The mobile router must be configured to receive SNMP linkUp and linkDown traps from the WMIC and can then make roaming decisions based on the type of trap received.

Mobile Router Processing of linkUp Traps

When a linkUp trap is received on a DHCP roaming interface, the mobile router interface will either renew the current IP address or acquire a new IP address as quickly as possible. If the interface already has a DHCP-acquired IP address, the mobile router will attempt to renew it first. If renewal fails, the interface will attempt to acquire a new IP address.

If a DHCP interface is without an IP address, DHCP address acquisition begins. Address "discovery" attempts are repeated at increasing intervals (up to 60 seconds) and continue until an address is acquired. During address discovery, the interface is "IP-enabled" and IP packets can be processed. This means that foreign agent CoA advertisements can be heard and Mobile IP registration can take place, even though the interface does not have an IP address.

The new **ip dhcp client mobile renew** command allows you to configure the number of renewal attempts and the interval between attempts for renewing the current IP address that was acquired through DHCP. The configured values override any default values.

For roaming purposes, the roaming interface treats a linkUp trap event the same as if the roaming interface just came up. For example, solicits are sent, if foreign agent CoA-enabled, and the mobile router determines if this interface, compared to other roaming interfaces, should register. Dynamic address acquisition can trigger a DCCoA registration.

If the interface is already registered when the linkUp trap arrives and nothing else has changed that affects the registration decision, the mobile router will retain the existing registration.

Mobile Router Processing of linkDown Traps

Receipt of a valid linkDown trap starts a new, configurable reassociation hold-down timer. The purpose of this timer is to delay the mobile router's response to the trap, which is typically an attempt to register on the next best interface, for a period of time long enough for the WMIC to reassociate with another bridge or access point (AP). The mobile router remains registered during this hold-down period, foreign agent data is retained, and the mobile router interface keeps any DHCP-acquired IP address. The hold-down timer should be set to the maximum time it should take the WMIC to re-establish wireless connectivity while roaming between adjacent bridges or APs.

If a linkUp trap arrives before the hold-down timer expires, the mobile router remains registered and foreign agent data is retained. Solicits are sent to find foreign agents and the DHCP IP address renewal and discovery process begins. If the WMIC has roamed to an AP on the same subnet, address renewal should succeed.

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

Benefits of Mobile Router DHCP Support for DCCoA and FA Processing

This feature allows a mobile router to roam to foreign networks where foreign agents may or may not be deployed and where IP addresses are obtained dynamically via DHCP. The SNMP trap capability permits the Cisco 3200 Series Mobile Access Router with a WMIC to respond to changes in the WLAN link status.

How to Configure Mobile Router DHCP Support for DCCoA

Enabling DHCP Support for DCCoA Processing on a Mobile Router Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address dhcp**
5. **ip dhcp client mobile renew count** *number* **interval** *msec*
6. **ip mobile router-service roam**
7. **ip mobile router-service collocated** [**ccoa-only**]
8. **ip mobile router-service hold-down reassociate** *msec*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address dhcp** **Example:** `Router(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP. • DHCP address acquisition time can be reduced by turning off the pings normally sent out by the DHCP server to verify that the IP address is not in use. If using a Cisco IOS router as a DHCP server, use the **ip dhcp ping packets** *number*commandand set the *number* argument to 0 (zero).

	Command or Action	Purpose
Step 5	**ip dhcp client mobile renew count** *number* **interval** *msec* **Example:** `Router(config-if)# ip dhcp client mobile renew count 4 interval 25`	(Optional) Configures the number of renewal attempts and the interval between attempts for renewing the current IP address acquired by DHCP. • By default the interface will attempt to renew its address twice and wait 50 milliseconds between attempts. You only need to use this command if you want to adjust the number of attempts or the interval between attempts.
Step 6	**ip mobile router-service roam** **Example:** `Router(config-if)# ip mobile router-service roam`	Enables roaming on an interface.
Step 7	**ip mobile router-service collocated** [**ccoa-only**] **Example:** `Router(config-if)# ip mobile router-service collocated`	Enables CCoA processing on a mobile router interface. • The interface will first solicit foreign agent advertisements and register with a foreign agent CoA if an advertisement is heard. If no advertisements are received, CCoA registration is attempted. • The **ccoa-only** keyword enables the interface to use CCoA processing only.
Step 8	**ip mobile router-service hold-down reassociate** *msec* **Example:** `Router(config-if)# ip mobile router-service hold-down reassociate 2000`	(Optional) Specifies the delay, after receiving a linkDown trap, that the mobile router waits for a linkUp trap. • The default is 1000 msec. The range is from 0 to 5000 seconds. • This reassociate hold-down period is the interval of time (in milliseconds) that the mobile router will wait, after receiving an SNMP linkDown trap, for a linkUp trap from the WMIC indicating that the wireless link is available for use.

Configuring SNMP on the Mobile Router

If a Cisco 3200 Series Mobile Access Router is using a WMIC, the router must be configured for SNMP. The WMIC uses SNMP trap messages to signal the mobile router that the WLAN is either up or down. See the Configuration Guide for the Cisco 3200 Series Mobile Access Router for additional information on how to configure SNMP traps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server engineID remote** *remote-ip-address* *remote-engineID-string*
4. **snmp-server user** *username group-name* **remote** *remote-ip-address* **v3**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server engineID remote** *remote-ip-address* *remote-engineID-string* **Example:** `Router(config)# snmp-server engineID remote 172.21.58.1 800000090300000F23AD8F30`	Specifies the SNMP engine ID of a remote SNMP device.
Step 4	**snmp-server user** *username group-name* **remote** *remote-ip-address* **v3** **Example:** `Router(config)# snmp-server user labusr labgrp remote 172.21.58.1 v3`	Configures a new user to an SNMP group.

Verifying the Dynamic CCoA Configuration

To verify the dynamic CCoA configuration, perform the following steps.

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for Mobile Router DHCP Support for DCCoA

Mobile Router DCCoA Acquired Through DHCP Example

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

Mobile Router

```
! This is the roaming interface using DCCoA
interface FastEthernet0
 ip address dhcp
 ip dhcp client mobile renew count 3 interval 20
 ip mobile router-service roam
 ip mobile router-service collocated
 ip mobile router-service hold-down reassociate 2000
!
! Receive v1 or v2 traps
snmp-server community public RO
snmp-server enable traps tty
!
! Receive v3 traps
snmp-server engineID remote 85.85.85.3 1234
snmp-server user labusr labgrp remote 85.85.85.2 v3 auth md5 <SNMP user password on WGB
>
snmp-server group labgrp v3 auth
```

Additional References

The following sections provide references related to the Mobile Router DHCP Support for DCCoA and FA Processing feature.

Related Documents

Related Topic	Document Title
Cisco 3200 Series Mobile Access Router documentation	Configuration Guide for the Cisco 3200 Series Mobile Access Router
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3T
Mobile IP commands and configuration tasks related to mobile networks	Cisco Mobile Networks feature document, Release 12.2(4)T and 12.2(13)T
Static CCoA documentation	Mobile Networks Static Collocated Care-of Address feature document, Release 12.2(15)T

Related Topic	Document Title
Dynamic CCoA documentation	Mobile Networks Dynamic Collocated Care-of Address feature document, Release 12.3(4)T

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Command Reference

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

- **ip dhcp client mobile renew**
- **ip mobile router-service**
- **show ip mobile router agent**
- **show ip mobile router interface**

Glossary

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

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

DHCP --Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses and other configuration parameters dynamically so that addresses can be reused when hosts no longer need them.

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

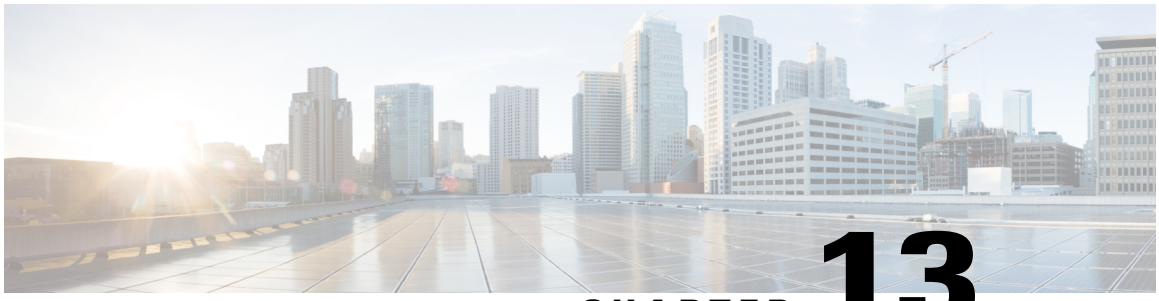
home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a mobility binding.

IPCP --IP Control Protocol. The protocol used to establish and configure IP over PPP.

PPP --Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is most commonly used for dial-up Internet access. Its features include address notification, authentication via CHAP or PAP, support for multiple protocols, and link monitoring.

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

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



CHAPTER 13

Prerequisites for MANET Enhancements to PPPoE for Router-to-Radio Links

To use the PPP over Ethernet (PPPoE) and virtual multipoint interface (VMI) features described in this document, a radio device that implements the PPPoE functionality enhancements described in the RFC 2516 and RFC 5578 is required.

Open Shortest Path First (OSPF) enhancements are not tied to the PPPoE/VMI implementations, and do not require such radio devices.

Information About MANET Enhancements to PPPoE for Router-to-Radio Links

About MANETs

Mobile Ad Hoc Networks (MANETs) for device-to-radio communications address the challenges faced when merging IP routing and mobile radio communications in ad hoc networking applications:

- Optimal route selection based on Layer 2 feedback from the radio network
- Faster convergence when nodes join and leave the network because devices are able to respond faster to network topology changes
- Efficient integration of point-to-point, directional radio topologies with multihop routing

- Flow-controlled communications between each radio and its partner device enables applications such as voice and video to work better because outages caused by moving links are reduced or eliminated. Sessions are more stable and remain active longer

Through the device-to-radio link, the radio can inform the device immediately when a node joins or leaves, and this enables the device to recognize topology changes more quickly than if it had to rely on timers. Without this link-status notification from the radio, the device would likely time out while waiting for traffic. The link-status notification from the radio enables the device to respond faster to network topology changes. Metric information regarding the quality of a link is passed between the device and radio, enabling the device to more intelligently decide on which link to use.

With the link-status signaling provided by the device-to-radio link, applications such as voice and video work better because outages caused by topology changes are reduced or eliminated. Sessions are more stable and remain active longer.

Cross-layer feedback for device-to-radio integration of Radio-Aware Routing (RAR) takes advantage of the functions defined in RFC 5578. The RFC 5578 is an Internet Engineering Task Force (IETF) standard that defines PPP over Ethernet (PPPoE) extensions for Ethernet-based communications between a device and a mobile radio, that operates in a variable-bandwidth environment and has limited buffering capabilities. These extensions provide a PPPoE session-based mechanism for sharing radio network status such as link-quality metrics and establishing flow control between a device and an RAR-compliant radio.

An RAR-compliant radio initiates a Layer 2 PPPoE session with its adjacent device on behalf of every device and radio neighbor discovered in the network. These Layer 2 sessions are the means by which radio network status for each neighbor link is reported to the device. The radio establishes the correspondence between each PPPoE session and each link to a neighbor.

Routing Challenges for MANETs

Mobile Ad Hoc Networks (MANETs) enable users deployed in areas with no fixed communications infrastructure to access critical voice, video, and data services. For example, soldiers in the field can employ unified communications, multimedia applications, and real-time information dissemination to improve situational awareness and respond quickly to changing battlefield conditions. Disaster managers can use video conferences, database access, and collaborative tools to coordinate multiagency responses within an Incident Command System (ICS) framework. For event planners and trade show managers, MANETs represent a cost-effective way to accommodate mobile end users on a short-term basis.

In MANET environments, highly mobile nodes communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network device, with the two devices interconnected over an Ethernet. Because these nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET becomes a challenge because the state of a node can change well before the event is detected by the normal timing mechanisms of the routing protocol.

Radio link quality in a MANET can vary dramatically because it can be affected by a variety of factors such as noise, fading, interference, and power fluctuation. As a result, avoiding congestion and determining optimal routing paths also pose significant challenges for the device network.

Directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multihop, multipoint device environments because it increases the size of each device's topology database and reduces routing efficiency.

Effective networking in a MANET environment therefore requires mechanisms by which

- Devices and radios can interoperate efficiently, and without impacting operation of the radio network.

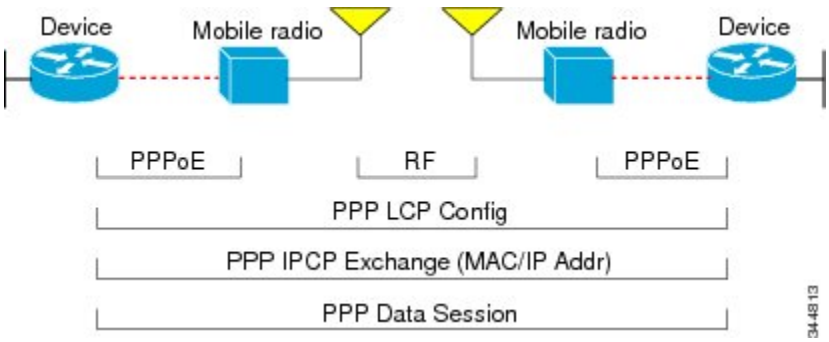
- Radio point-to-point and device point-to-multipoint paradigms can be rationalized.
- Radios can report status to devices for each link and each neighbor.
- Devices can use this information to optimize routing decisions.

PPPoE Interfaces for Mobile Radio Communications

The Mobile Ad Hoc Network (MANET) implementation uses PPP over Ethernet (PPPoE) sessions to enable intranodal communications between a device and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (device-to-device). This is duplicated each time a radio establishes a new radio link. The virtual multipoint interface (VMI) on the device can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Underneath the VMI are virtual access interfaces that are associated with each of the PPP and PPPoE connections.

A PPPoE session is established between a device and a radio on behalf of every other device and radio neighbor located in the MANET. These Layer 2 sessions are the means by which radio network status gets reported to the Layer 3 processes in the device. The figure below shows the PPPoE session exchange between mobile devices and directional radios in a MANET network.

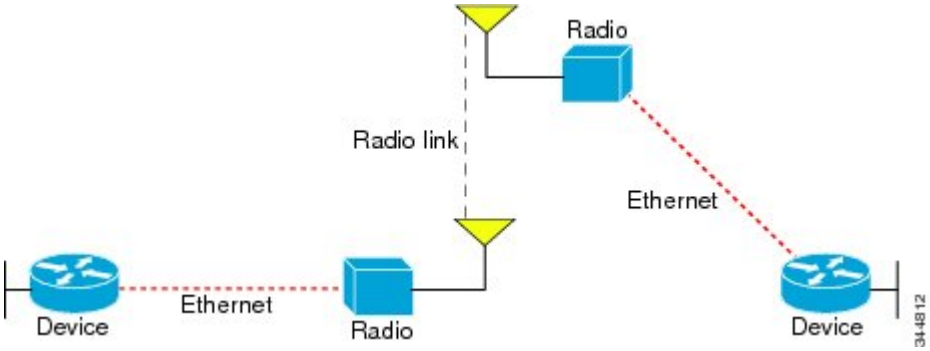
Figure 10: PPPoE Session Exchange Between Mobile Devices and Directional Radios



This capability requires that a Radio-Aware Routing (RAR)-compliant radio be connected to a device through Ethernet. The device always considers the Ethernet link to be up. If the radio side of the link goes down, the device waits until a routing update timeout occurs to declare the route down and then updates the routing table. The figure below shows a simple device-to-radio link topology.

The routing protocols optimized for VMI PPPoE are Enhanced Interior Gateway Routing Protocol (EIGRP) (IPv4, IPv6) and Open Shortest Path First version 3 (OSPFv3) for IPv4 and IPv6.

Figure 11: Device-to-Radio Link



Benefits of Virtual Multipoint Interfaces

The virtual multipoint interface (VMI) provides services that map outgoing packets to the appropriate PPP over Ethernet (PPPoE) sessions based on the next-hop forwarding address for that packet. The VMI also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through the VMI in aggregate mode, VMI replicates the packet and sends it through the virtual access interfaces to each of its neighbors.

Directional radios are frequently used in applications that require greater bandwidth, increased power-to-transmission range, or reduced probability of detection. These radios operate in a point-to-point mode and generally have no broadcast capability. However, the routing processes in Mobile Ad Hoc Networks (MANETs) operate most efficiently because the network link is treated as point-to-multipoint, with broadcast capability. For the device, modeling the MANET as a collection of point-to-point nodes has a dramatic impact on the size of its internal database.

The VMI within the device can aggregate all of the per-neighbor PPPoE sessions from the radio Ethernet connection. The VMI maps the sessions to appear to Layer 3 routing protocols and applications as a single point-to-multipoint, multiaccess, broadcast-capable network. However, the VMI preserves the integrity of the PPPoE sessions on the radio side so that each point-to-point connection can have its own quality of service (QoS) queue.

The VMI also relays the link-quality metric and neighbor up/down signaling from the radio to the routing protocols. The VMI signals are used by the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6 neighbors and the Open Shortest Path First version 3 (OSPFv3) for IPv6 neighbors.

IPv6 Address Support on VMIs

You can configure virtual multipoint interfaces (VMIs) with IPv6 addresses only, IPv4 addresses only, or both IPv4 and IPv6 addresses.

IPv6 addresses are assigned to individual device interfaces and enable the forwarding of IPv6 traffic globally on the device. By default, IPv6 addresses are not configured and IPv6 routing is disabled.

Note The *ipv6-address* argument in the **ipv6 address** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The */prefix-length* argument in the **ipv6 address** command is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) A slash mark must precede the decimal value.

Restrictions for IPv6 Addressing

The **ipv6 address** or the **ipv6 address eui-64** command can be used to configure multiple IPv6 global addresses within the same prefix on an interface. Multiple IPv6 link-local addresses on an interface are not supported.

OSPFv3 Address Families

The Open Shortest Path First version 3 9OSPFv3) address family feature is implemented according to RFC 5838 and enables the concurrent routing of IPv4 and IPv6 prefixes.

When this feature is enabled with Mobile Ad Hoc Networks (MANETs), IPv6 packets are routed in mobile environments over OSPFv3 using IPv4 or IPv6 addresses.

For configuration details, see the *IP Routing: OSPF Configuration Guide*.

Neighbor Up and Down Signaling for OSFPv3 and EIGRP

Mobile Ad Hoc Networks (MANETs) are highly dynamic environments. Nodes might move into, or out of, radio range at a fast pace. Each time a node joins or leaves, the network topology must be logically reconstructed by the devices. Routing protocols normally use timer-driven hello messages or neighbor timeouts to track topology changes, but MANETs reliance on these mechanisms can result in unacceptably slow convergence.

The neighbor up/down signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the device each time a link to another neighbor is established or terminated by the creation and termination of PPP over Ethernet (PPPoE) sessions. In the device, the routing protocols (Open Shortest Path First version 3 [OSPFv3] or Enhanced Interior Gateway Routing Protocol [EIGRP]) respond immediately to these signals by expediting formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the device immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high-speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When virtual multipoint interfaces (VMIs) with PPPoE are used and a partner node has left or a new one has joined, the radio informs the device immediately of the topology change. Upon receiving the signal, the device immediately declares the change and updates the routing tables. The signaling capability provides these advantages:

- Reduces routing delays and prevents applications from timing out
- Enables network-based applications and information to be delivered reliably and quickly over directional radio links

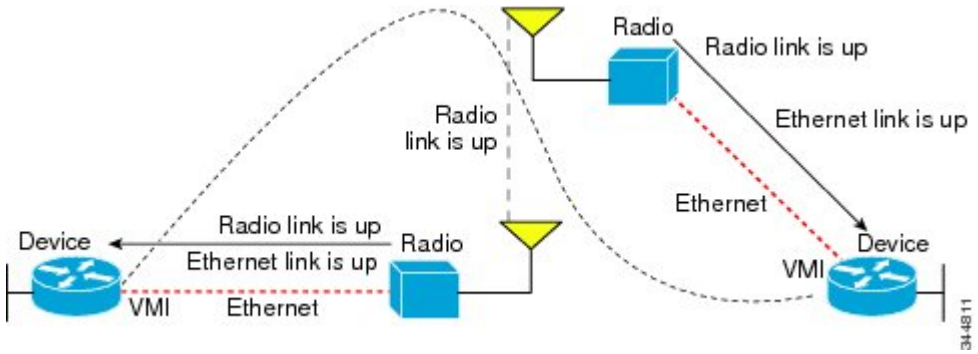
- Provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queueing and buffering
- Provides consistent quality of service for networks with multiple radios

The messaging allows for flexible rerouting when necessary because of these factors:

- Noise on the radio links
- Fading of the radio links
- Congestion of the radio links
- Radio link power fade
- Utilization of the radio

The figure below shows the signaling sequence that occurs when radio links go up and down.

Figure 12: Up and Down Signaling Sequence



PPPoE Credit-based and Metric-based Scaling and Flow Control

Each radio initiates a PPP over Ethernet (PPPoE) session with its local device as soon as the radio establishes a link to another radio. Once the PPPoE sessions are active for each node, a PPP session is then established end-to-end (device-to-device). This process is duplicated each time a radio establishes a new link.

The carrying capacity of each radio link might vary due to location changes or environmental conditions, and many radio transmission systems have limited buffering capabilities. To minimize the need for packet queueing in the radio, PPPoE protocol extensions enable the device to control traffic buffering in congestion situations. Implementing flow-control on these device-to-radio sessions allows use of quality of service (QoS) features such as fair queueing.

The flow-control solution utilizes a credit-granting mechanism documented in RFC 5578. When the PPPoE session is established, the radio can request a flow-controlled session. If the device acknowledges the request, all subsequent traffic must be flow controlled. If a flow-control session is requested and cannot be supported by the device, the session is terminated. Typically, both the radio and the device initially grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits are granted. Credits can be added incrementally over the course of a session.

Metrics scaling is used with high-performance radios that require high-speed links. The radio can express the maximum and current data rates with different scaler values. Credit scaling allows a radio to change the default credit grant (or scaling factor) of 64 bytes to its default value. You can display the maximum and current data rates and the scalar value set by the radio in the **show vmi neighbor detail** command output.

How to Configure MANET Enhancements to PPPoE for Router-to-Radio Links

Configuring a Subscriber Profile for PPPoE Service Selection

For virtual multipoint interfaces (VMIs) to work, you must configure a subscriber profile for PPP over Ethernet (PPPoE) service selection. In this task, you configure the PPPoE service name, which is used by Radio-Aware Routing (RAR)-compliant radio PPPoE clients to connect to the PPPoE server.

All PPPoE service names used for MANET implementations *must* begin with *manet_radio* for use with VMI and RFC 5578 features. Example service names are manet_radio and manet_radio_satellite.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **pppoe service manet_radio**
5. **exit**
6. **subscriber authorization enable**
7. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**subscriber profile** *profile-name* **Example:** `Device(config)# subscriber profile manet`	Enters subscriber profile configuration mode.
Step 4	**pppoe service manet_radio** **Example:** `Device(config-sss-profile)# pppoe service manet_radio`	Adds a PPPoE MANET radio service name to a subscriber profile to enable the use of the VMI.
Step 5	**exit** **Example:** `Device(config-sss-profile)# exit`	Returns to global configuration mode.
Step 6	**subscriber authorization enable** **Example:** `Device(config)# subscriber authorization enable`	Enable Subscriber Service Switch type authorization. • This command is required when virtual private dialup networks (VPDNs) are not used.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Assigning the Subscriber Profile to a PPPoE Profile

Perform this required task to assign a subscriber profile to a PPP over Ethernet (PPPoE) profile. In this configuration, the BBA group name should match the subscriber profile name previously defined in the subscriber profile. In this case, the profile name used as the service name is manet_radio.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Device(config)# bba-group pppoe group1`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Device(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Device(config-bba-group)# service profile subscriber-group1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. • Use the **refresh** *minutes* keyword and argument to cause the cached PPPoE configuration to time out after a specified number of minutes.
Step 6	**end** **Example:** `Device(config-bba-group)# end`	(Optional) Returns to privileged EXEC mode.

Troubleshooting Tips

Use the **show pppoe session** and the **debug pppoe** commands to troubleshoot PPP over Ethernet (PPPoE) sessions.

Enabling PPPoE Sessions on an Interface

Perform this required task to enable PPP over Ethernet (PPPoE) sessions on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pppoe enable** [**group** *group-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 3/1`	Specifies an interface and enters interface configuration mode. • Ethernet, Fast Ethernet, Gigabit Ethernet, VLANs, and VLAN subinterfaces can be used.
Step 4	**pppoe enable** [**group** *group-name*] **Example:** `Device(config-if)# pppoe enable group bba1`	Enables PPPoE sessions on an interface or subinterface.
Step 5	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Creating a Virtual Template for IPv4 and IPv6

Perform this optional task to create a virtual template for IPv4 and IPv6. You use the virtual template interface to dynamically clone configurations for each virtual access interface created for a virtual multipoint interface (VMI) neighbor.

Before You Begin

Cisco recommends that, when using the virtual template, you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy radio frequency (RF) link.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. Perform steps 5 and 8 if you are using IPv4. Perform steps 6, 7, and 8 if you are using IPv6. If you are using both, perform steps 5, 6, 7, and 8.
5. **ip unnumbered** *interface-type interface-number*
6. **ipv6 enable**
7. **ipv6 unnumbered** *interface-type interface-number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Creates a virtual template, and enters interface configuration mode.
Step 4	Perform steps 5 and 8 if you are using IPv4. Perform steps 6, 7, and 8 if you are using IPv6. If you are using both, perform steps 5, 6, 7, and 8.	--

	Command or Action	Purpose
	Example: **Example:**	
Step 5	**ip unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on an interface without assigning an explicit IP address to the interface.
Step 6	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the interface.
Step 7	**ipv6 unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ipv6 unnumbered vmi I`	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
Step 8	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Creating a VMI for EIGRP IPv4

Perform this optional task to create the VMI for the Enhanced Interior Gateway Routing Protocol for IPv4 (EIGRP IPv4) and associate it with the interface on which PPP over Ethernet (PPPoE is enabled).

Before You Begin

When you create a virtual multipoint interface (VMI), assign the IPv4 address to that VMI definition.

The radio alerts the device with PADT messages that the Layer-2 radio frequency (RF) connection is no longer alive. Cisco recommends that you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

This configuration includes quality of service (QoS) fair queueing and a service policy applied to the VMI. Make certain that any fair queueing left over from any previous configurations is removed before applying the new policy map to the virtual template in the VMI configuration.

Note Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **no virtual-template subinterface**
5. **policy-map** *policy-mapname*
6. **class class-default**
7. **fair-queue**
8. **exit**
9. **exit**
10. **interface virtual-template** *number*
11. **ip unnumbered** *interface-type interface-number*
12. **service-policy output** *policy-mapname*
13. **no keepalive**
14. **interface** *type number*
15. **ip address** *address mask*
16. **no ip redirects**
17. **no ip split-horizon eigrp** *autonomous-system-number*
18. **physical-interface** *type number*
19. **exit**
20. **router eigrp** *autonomous-system-number*
21. **network** *network-number ip-mask*
22. **redistribute connected**
23. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip routing** **Example:** `Device(config)# ip routing`	Enables IP routing on the device.
Step 4	**no virtual-template subinterface** **Example:** `Device(config)# no virtual-template subinterface`	Disables the virtual template on the subinterface.
Step 5	**policy-map** *policy-mapname* **Example:** `Device(config)# policy-map fair-queue`	Enters QoS policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 6	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • Enters Qos policy-map class configuration mode.
Step 7	**fair-queue** **Example:** `Device(config-pmap-c)# fair-queue`	Enables weighted fair queueing (WFQ) on the interface.
Step 8	**exit** **Example:** `Device(config-pmap-c)# exit`	Returns to QoS policy-map configuration mode.
Step 9	**exit** **Example:** `Device(config-pmap)# exit`	Returns to global configuration mode.
Step 10	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

	Command or Action	Purpose
Step 11	**ip unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on a serial interface without assigning an explicit IP address to the interface.
Step 12	**service-policy output** *policy-mapname* **Example:** `Device(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface, virtual circuit (VC), or to an output interface or VC. • The policy map is as the service policy for that interface or VC.
Step 13	**no keepalive** **Example:** no `Device(config-if)# no keepalive`	Turns off PPP keepalive messages to the interface.
Step 14	**interface** *type number* **Example:** `Device(config-if)# interface vmi 1`	Specifies the number of the VMI.
Step 15	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 16	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Disables the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco software is forced to resend a packet through the same interface on which it was received.
Step 17	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ip split-horizon eigrp 101`	Disables the split horizon mechanism for the specified session.
Step 18	**physical-interface** *type number* **Example:** `Device(config-if)# physical-interface FastEthernet 0/1`	Creates the physical subinterface to be associated with the VMIs on the device.

	Command or Action	Purpose
Step 19	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 20	**router eigrp** *autonomous-system-number* **Example:** `Device(config)# router eigrp 100`	Enables EIGRP routing on the device, identifies the autonomous system number, and enters router configuration mode.
Step 21	**network** *network-number ip-mask* **Example:** `Device(config-router)# network 209.165.200.225 255.255.255.224`	Identifies the EIGRP network.
Step 22	**redistribute connected** **Example:** `Device(config-router)# redistribute connected`	Redistributes routes from one routing domain into another routing domain.
Step 23	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Creating a VMI for EIGRP IPv6

Perform this optional task to create the VMI for the Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRP IPv6) and associate it with the interface on which PPP over Ethernet (PPPoE) is enabled.

Before You Begin

When you create a virtual multipoint interface (VMI), assign the IPv6 address to that VMI definition.

The radio alerts the device with PADT messages that the Layer-2 radio frequency (RF) connection is no longer alive. Cisco recommends that if you turn off the PPP keepalive messages to make CPU usage more efficient and help to avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

This configuration includes quality of service (QoS) fair queueing and a service policy applied to the VMI. Make certain that any fair queueing left over from any previous configurations is removed before applying the new policy map to the virtual template in the VMI configuration.

Note Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no virtual-template subinterface**
4. **ipv6 unicast-routing**
5. **ipv6 cef**
6. **policy-map** *policy-mapname*
7. **class class-default**
8. **fair-queue**
9. **exit**
10. **exit**
11. **interface virtual-template** *number*
12. **ipv6 enable**
13. **no keepalive**
14. **service-policy output** *policy-mapname*
15. **interface** *type number*
16. **ipv6 address** *address*/*prefix-length*
17. **ipv6 enable**
18. **ipv6 eigrp** *as-number*
19. **no ipv6 redirects**
20. **no ipv6 split-horizon eigrp** *as-number*
21. **physical-interface** *type number*
22. **no shutdown**
23. **ipv6 router eigrp** *as-number*
24. **redistribute connected**
25. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no virtual-template subinterface** **Example:** `Device(config)# no virtual-template subinterface`	Disables the virtual template on the subinterface.
Step 4	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables IPv6 unicast routing.
Step 5	**ipv6 cef** **Example:** `Device(config)# ipv6 cef`	Enables IPv6 Cisco Express Forwarding on the device
Step 6	**policy-map** *policy-mapname* **Example:** `Device(config-pmap)# policy-map fair-queue`	Enters QoS policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 7	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • Enters QoS policy-map class configuration mode.
Step 8	**fair-queue** **Example:** `Device(config-pmap-c)# fair-queue`	Enables weighted fair queueing (WFQ) on the interface.
Step 9	**exit** **Example:** `Device(config-pmap-c)# exit`	Returns to QoS policy-map configuration mode.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Device(config-pmap)#  exit`	Returns to global configuration mode.
Step 11	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 12	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 routing on the virtual template.
Step 13	**no keepalive** **Example:** `Device(config-if)# no keepalive`	Turns off PPP keepalive messages to the virtual template.
Step 14	**service-policy output** *policy-mapname* **Example:** `Device(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface, virtual circuit (VC), or to an output interface or VC. • The policy map is as the service policy for that interface or VC.
Step 15	**interface** *type number* **Example:** `Device(config-if)# interface vmi 1`	Creates a VMI.
Step 16	**ipv6 address** *address*/*prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address for the interface.
Step 17	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 routing on the interface.

	Command or Action	Purpose
Step 18	**ipv6 eigrp** *as-number* **Example:** `Device(config-if)# ipv6 eigrp 1`	Enables the EIGRP for IPv6 on a specified interface and specifies the autonomous system number.
Step 19	**no ipv6 redirects** **Example:** `Device(config-if)# no ipv6 redirects`	Disables the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if the software is forced to resend a packet through the same interface on which the packet was received
Step 20	**no ipv6 split-horizon eigrp** *as-number* **Example:** `Device(config-if)# no ipv6 split-horizon eigrp 100`	Disables the split horizon for EIGRP IPv6. • Associates this command with a specific EIGRP autonomous system number.
Step 21	**physical-interface** *type number* **Example:** `Device(config-if)# physical-interface FastEthernet 1/0`	Creates the physical subinterface to be associated with the VMIs on the device.
Step 22	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface or prevents the interface from being shut down.
Step 23	**ipv6 router eigrp** *as-number* **Example:** `Device(config-if)# ipv6 router eigrp 100`	Places the device in router configuration mode, creates an EIGRP routing process in IPv6, and allows you to enter additional commands to configure this process.
Step 24	**redistribute connected** **Example:** `Device(config-router)# redistribute connected`	Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running. • Redistributes IPv6 routes from one routing domain into another routing domain.
Step 25	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Verifying the VMI Configuration

You can use the following commands to verify the virtual multipoint interface (VMI) configuration:

- **show pppoe session all**
- **show interface vmi**
- **show vmi neighbors**
- **show vmi neighbors detail**
- **show ip eigrp interfaces**
- **show ip eigrp neighbors**
- **show ipv6 eigrp interfaces**
- **show ipv6 eigrp neighbors**
- **show ipv6 ospf interface**

Configuration Examples for MANET Enhancements to PPPoE for Router-to-Radio Links

Example: Basic VMI PPPoE Configuration with EIGRP IPv4

The following example shows the basic virtual multipoint interface (VMI) PPP over Ethernet (PPPoE) configuration with the Enhanced Interior Gateway Routing Protocol for IPv4 (EIGRP IPv4) as the routing protocol. This configuration includes one VMI.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password test
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
```

```
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
```

```
 ip unnumbered vmi1
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.226 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
!
interface vmi1
 ip address 209.165.200.226 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 dampening-change 50
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Example: Basic VMI PPPoE Configuration with EIGRP IPv6

The following example shows the basic requirements for configuring a virtual multipoint interface (VMI) that uses the Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRP IPv6) as the routing protocol. It includes one VMI.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
ip cef
!
```

```
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
!
!
archive
 log config
!
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
!
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
!
interface Loopback1
 ip address 209.165.200.226 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
```

```
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 physical-interface FastEthernet0/0
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
```

```
line aux 0
line vty 0 4
 login
!
end
```

Example: VMI PPPoE Configuration with EIGRP for IPv4 and IPv6

The following examples show how to configure the virtual multipoint interface (VMI) for PPP over Ethernet (PPPoE) using the Enhanced Interior Gateway Routing Protocol (EIGRP) as the IP routing protocol when you have both IPv4 and IPv6 addresses configured on the interface. This configuration includes one VMI. Though EIGRP allows you to use the same autonomous system (AS) number on an IPv4 EIGRP process and on an IPv6 process, we recommend using a unique AS number for each process for clarity.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
```

```
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
```

```
interface vmi1
 ip address 209.165.200.225 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 10
 dampening-interval 30
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.225 255.255.255.224
 network 209.165.200.226 255.255.255.224
 auto-summary
!
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Example: VMI Configuration Using Multiple Virtual Templates

The following example shows how to configure the virtual multipoint interface (VMI) by using multiple virtual templates. This example shows two VMIs, each with a different service name.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
!
subscriber profile router1_ground
```

```
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.225 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Example: PPPoE Configuration

In the following example, the subscriber profile uses a predefined string manet_radio to determine whether an inbound PPP over Ethernet (PPPoE) session is coming from a device that supports the virtual multipoint interface (VMI). All IP definitions are configured on the VMI rather than on the Fast Ethernet or virtual-template interfaces; when those interfaces are configured, do not specify either an IP address or an IPv6 address.

No IP address is specified, and IPv6 is enabled by default on the VMI:

```
subscriber profile list1
  pppoe service manet_radio
  subscriber authorization enable
!
bba-group pppoe bba1
  virtual-template 1
  service profile list1
!
interface FastEthernet0/1
  no ip address
  pppoe enable group bba1
!
interface Virtual-Template 1
  no ip address
  no peer default ip-address
!
interface vmi 1
  no ip address
  physical-interface FastEthernet0/1
```

Example: Configuring Two VMIs and Two Virtual Templates

The following example shows a configuration that includes two virtual multipoint interfaces (VMIs), two virtual templates, and two service names. You can configure multiple virtual template interfaces for your VMI PPP over Ethernet (PPPoE) connections. The selection of which virtual template to use is predicated on the service name sent by the radio during PPPoE session establishment.

In this example, any PPPoE request for a session (presentation of a PPPoE Active Discovery Initiate [PADI] packet) with the service name of “manet_radio_ground” uses Virtual-Template1 as the interface to be cloned. Conversely, any PADI presented by the radio with the service name of “manet_radio_satellite” uses Virtual-Template2.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
```

```
!
subscriber profile router1_ground
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
 policy-map FQ
 class class-default
 fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 ip unnumbered vmi2
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.226 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.227 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
PPPoE and virtual templates	*Dial Configuration Guide* Cisco IOS Dial Technologies Command Reference
PPPoE configuration and commands	*Broadband Access Aggregation and DSL Configuration Guide* Cisco IOS Broadband Access Aggregation and DSL Command Reference
IPv6 addressing and basic connectivity	*IPv6 Addressing and Basic Connectivity Configuration Guide* (part of the IPv6 Configuration Guide Library)
IPv6 commands	Cisco IOS IPv6 Command Reference
Open Shortest Path First version 3 (OSPFv3) address families	*IP Routing: OSPF Configuration Guide*

RFCs

RFC	Title
RFC 2373	*IP Version 6 Addressing Architecture*
RFC 2516	*A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 5578	*PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics*
RFC 5838	*Support of Address Families in OSPFv3*

Technical Assistance

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

Feature Information for MANET Enhancements to PPPoE for Router-to-Radio Links

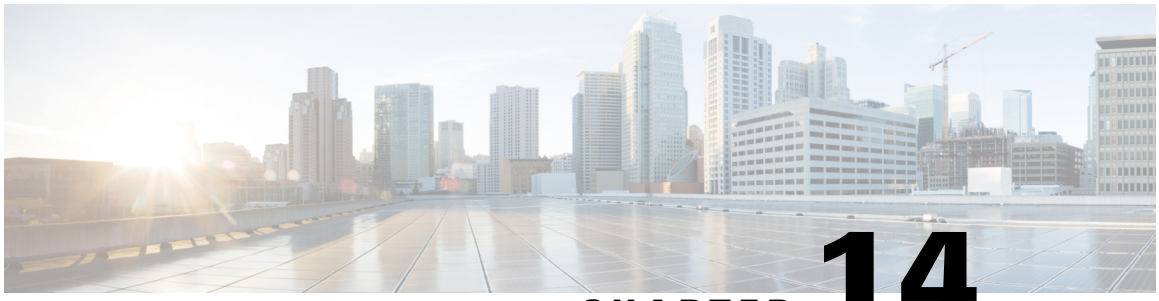
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

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

Table 3: Feature Information for MANET Enhancements to PPPoE for Router-to-Radio Links

Feature Name	Releases	Feature Information
MANET Enhancements to PPPoE for Router-to-Radio Links	12.4(15)XF 12.4(15)T 15.0(1)M	The MANET Enhancements to PPPoE for Router-to-Radio Links feature provides credit-based flow control and link-quality metrics over mobile radio links. Credit-based flow control provides in-band and out-of-band credit grants in each direction. Link-quality metrics report link performance statistics that are then used to influence routing. The following commands were introduced or modified: **show pppoe session**, **show vmi neighbors**.

Feature Name	Releases	Feature Information
Radio Aware Routing RFC 5578	15.1(3)T	Radio-Aware Routing incorporates RFC 5578 updates for interfacing Cisco devices to high-performance radios through PPP over Ethernet (PPPoE). The following commands were introduced or modified: **show vmi neighbors**.



CHAPTER 14

OSPFv3 Extensions for Mobile Ad Hoc Networks

Open Shortest Path First version 3 (OSPFv3) Extensions optimize OSPFv3 behavior for more efficient routing in Mobile Ad Hoc Networks (MANETs). The OSPFv3 extensions improve routing efficiency and reduce overhead traffic in MANET environments so that network clusters can scale to support more users. The OSPFv3 extensions boost performance for delay-sensitive, mission-critical voice, video, and data traffic, and it facilitates the integration of wireless MANETs with existing wire-line products.

Finding Feature Information

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

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

Prerequisites for OSPFv3 Extensions for MANETs

You must create the subscriber profile for PPP over Ethernet (PPPoE) service selection, assign the subscriber profile to a PPPoE profile, and enable PPPoE sessions on the interface. For details, see the "Mobile Ad Hoc Networks for Router-to-Radio Communications" module.

Information About OSPFv3 Extensions for MANETs

OSPFv3 Extensions Operation with MANETs

To optimize the use of OSPFv3 with MANETs, Cisco software implements extensions to OSPFv3 as defined in *draft-chandra-ospf-manet-ext-02* . The result is a well-understood routing protocol (OSPF) used in a network topology that is constantly changing and where bandwidth is limited.

OSPF is optimized in these ways:

- Tightly couples OSPFv3 with Radio Aware Routing (RAR)-compliant radios to provide faster convergence and reconvergence through neighbor presence indications and help determine accurate, real-time link metric costs.
- Minimizes OSPFv3 packet size by implementing incremental hellos.
- Minimizes the number of OSPFv3 packet transmissions by caching multicast link-state advertisements (LSAs).
- Implements optimized flooding (overlapping relay) functionality to minimize the number of flooded LSAs.
- Implements selective peering to reduce the OSPF network overhead by minimizing the number of redundant full adjacencies that an OSPF node maintains.

Radio-Aware Link-Metrics Tuning for OSPFv3

The RAR-compliant radio reports link-quality metrics to the router that are used by OSPFv3 as link metrics. You can fine-tune to adjust how these radio metrics are used by OSPFv3:

1. Configure how the radio-reported bandwidth, latency, resource, and relative link-quality metrics are converted to an OSPFv3 link cost.
2. Configure a hysteresis threshold on this resultant link cost to minimize the propagation of LSAs that report link-metric changes.

OSPFv3 receives raw radio-link data and computes a composite. In computing these metrics, you should consider these factors (see the figure "OSPF Cost Calculation for VMI Interfaces"):

- Maximum data rate--the theoretical maximum data rate of the radio link, in bytes per second
- Current data rate--the current data rate achieved on the link, in bytes per second
- Resources--a percentage (0 to100) that can represent the remaining amount of a resource (such as battery power)
- Latency--the transmission delay packets encounter, in milliseconds
- Relative link quality (RLQ)--a numeric value (0 to 100) representing relative quality, with 100 being the highest quality

You can weight metrics during the configuration process to emphasize or de-emphasize particular characteristics. For example, if throughput is a particular concern, you can weight the current data rate metric so that it is

factored more heavily into the composite metric. Similarly, you can omit a metric that is of no concern from the composite calculation.

Link metrics can change rapidly, often by very small degrees, which can result in a flood of meaningless routing updates. In a worst-case scenario, the network churns almost continuously as it struggles to react to minor variations in link quality. To alleviate this concern, you can use a tunable dampening mechanism to configure threshold values. Any metric change that falls below the threshold is ignored.

With the tunable hysteresis mechanism, you can adjust the threshold to the routing changes that occur when the router receives a signal that a new peer has been discovered, or that an existing peer is unreachable. The tunable metric is weighted and is adjusted dynamically to account for these characteristics:

- Current and maximum bandwidth
- Resources
- Latency
- Hysteresis

You can deconfigure individual weights and clear all weights so that the cost is returned to the default value for the interface type. Based on the routing changes that occur, the cost can be determined by the application of these metrics.

Dynamic Cost Metric for Virtual Multipoint Interfaces

The dynamic cost metric used for virtual multipoint interfaces (VMIs) is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). The dynamic cost is calculated using this formula:

OC = maximum-data-rate

S1 = ospfv3 *process-id* cost dynamic weight throughput (bandwidth component)

S2 = ospfv3 *process-id* cost dynamic weight resources (resources component)

S3 = ospfv3 *process-id* cost dynamic weight latency (latency component)

S4 = ospfv3 *process-id* cost dynamic weight L2-factor (L2 factor component)

Throughput = (current-data-rate)/(maximum-data-rate)

Router-dynamic cost = OC + (S1) + (S2) + (S3) + (S4)

For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword with the **throughput**, **resources**, **latency**, or **L2-factor** keyword with the **ospfv3 cost** command. Each of these weights has a default value of 100 percent and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPF cost.

Because cost components can change rapidly, you might need to dampen the number of changes to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument with the **ospfv3 cost** command to set a cost change threshold. Any cost change below this threshold is ignored.

You can use the **hysteresis** keyword to specify a hysteresis value based on the percentage of change of the currently stored value in the routing table for the peer.

Each time the router receives a new packet discovery quality (PADQ) packet from the radio for a peer, a new cost is calculated for it. The **hysteresis** keyword specifies the amount of change required before the router saves the new value.

The hysteresis percent calculated is performed as follows:

If the absolute value of (new_cost - saved_cost) is greater than (hysteresis_percent*saved_cost), then the new_cost is saved.

Because cost components can change rapidly, you might need to dampen the volume of changes to reduce network-wide churn. The recommended values for S2, S3, and S4 are based on network simulations that might reduce the rate of network changes. The recommended value for S1 is zero to eliminate this variable from the route cost calculation.

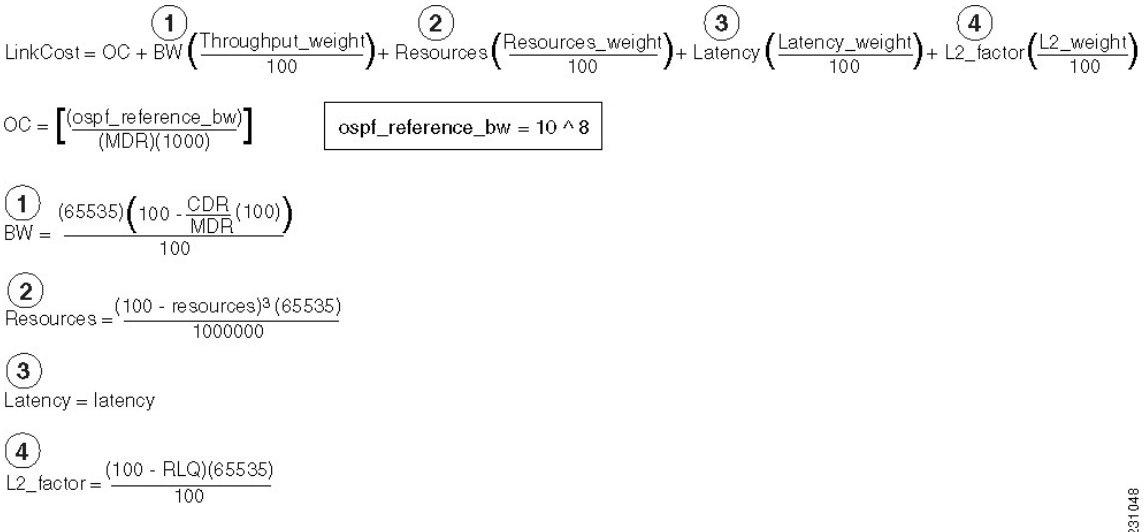
Each network might have unique characteristics that require different settings to optimize actual network performance, the table below lists the recommended cost settings intended as a starting point for optimizing an OSPFv3 network.

Table 4: Recommended Value Settings for OSPF Cost Metrics

Setting	Metric Command	Default Value	Recommended Value
S1	ospfv3 6 cost dynamic weight throughout	100	0
S2	ospfv3 6 cost dynamic weight resources	100	29
S3	ospfv3 6 cost dynamic weight latency	100	29
S4	ospfv3 6 cost dynamic weight L2-factor	100	29

The overall link cost is computed by using the formula shown in the figure below.

Figure 13: OSPF Cost Calculation for VMI Interfaces



To illustrate these settings, the following example shows how OSPF cost metrics might be defined for a VMI interface with one type of radio:

```
interface vmi1
ospfv3 6 cost dynamic weight throughput 0
ospfv3 6 cost dynamic hysteresis percent 10
ospfv3 6 cost dynamic weight resources 29
ospfv3 6 cost dynamic weight latency 29
ospfv3 6 cost dynamic hysteresis percent 10
ospfv3 6 cost dynamic weight L2-factor 29
```

Selective Peering

Selective peering reduces the OSPF network overhead by minimizing the number of redundant full adjacencies that an OSPF node maintains. Adjacencies to nodes that do not provide additional reachability can be kept in a two-way state. Selective peering reduces control-plane bandwidth utilization by reducing the number of database exchanges and routing updates.

Note Dataplane connectivity is not reduced when selective peering is enabled. User traffic flows over two-way links if they provide the best path through the network.

In the simplest example, selective peering determines if an adjacency should be formed when a new neighbor is discovered (a hello is received from a new neighbor). If the neighbor is not in the OSPF link state database, or if it is not reachable in the Shortest Path Tree (SPT), then the adjacency is formed. If the neighbor is in the OSPF link state database and is reachable, the neighbor is kept in the two-way state if the configured number of redundant paths to this neighbor is already formed.

Topology changes might cause the number of redundant paths to a given neighbor to fall below the configured level. When this occurs, selective peering can bring up adjacencies that were previously kept in the two-way state.

Selective peering takes link cost into consideration when determining which adjacencies to form. The objective is to have the reduced numbers of adjacencies formed over the lowest cost links. You can manually configure per-neighbor OSPF link costs, but with RAR-compliant radio interfaces, link costs are dynamically obtained from the radio through the VMI.

Selective Peering Link-Metrics Tuning

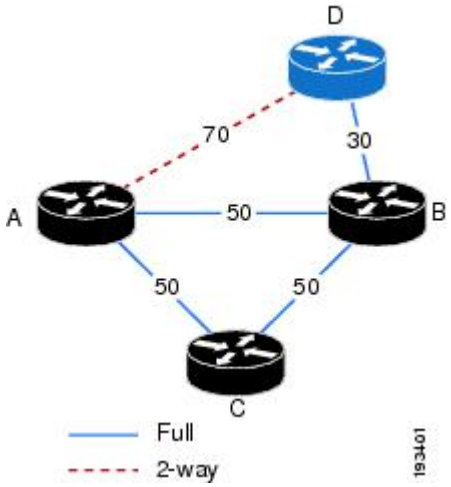
If the configured selective peering redundancy level is greater than 0, then at least two OSPFv3 control plane paths are maintained for every one hop neighbor. As new neighbors are discovered, full peering relationships are formed regardless of the link cost (as long as the cost satisfies the optionally configured minimum threshold specified in the **ospfv3 manet peering link-metrics** command).

As additional neighbors are brought to the full peering state to achieve the configured number of redundant paths to every neighbor, the router evaluates the path costs resulting from these new peering relationships to determine if they are incrementally better than the existing path costs. If they are not, the router keeps these links in a two-way state until other peering opportunities arise. The result is better path costs.

Consider the topology shown in the figure below. The configured redundancy level is 1 (the default), meaning that Router A attempts to maintain two paths to every one hop neighbor. Router A is in a full peering relationship with Router B and the link cost is 50. Router B is in a full peering relationship with Router D and the link cost is 30. Now Router D comes into radio range of Router A with a link cost of 70. Because the

number of paths from Router A to Router D is currently 1 (through Router B), Router A brings this relationship to the full state.

Figure 14: Selective Peering with Link Metrics



You can keep Routers A and D in a two-way state until the link cost between them improves, or until another router comes into range that has better link costs to both of them. This can be achieved by configuring a redundant path cost threshold. In the figure above, if a redundant path cost threshold of 20 is configured, then Routers A and D will not transition to the full state until their link cost falls below the current path cost of 80 (50 + 30) minus 20, or 60. Because the depicted path cost is 70, the routers remain in the two-way state.

How to Configure OSPFv3 Extensions for MANETs

Configuring OSPFv3 in MANETs for Radio-Aware Routing

Perform this required task to create the VMI interface for OSPFv3 and associate it with the interface on which PPPoE is enabled. For OSPFv3 to take advantage of radio feedback, you must configure OSPFv3 MANET on the VMI. By default, VMI uses neighbor presence and link-metric data from the radio.

After you complete this task, you must fine-tune RAR link metrics as described in the Fine-Tuning Radio-Aware Routing Link Metrics, on page 202.

Before You Begin

You must create a VMI interface and then assign the IPv6 or the IPv4 address to that VMI definition.

Note Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no virtual-template subinterface**
4. **ipv6 unicast-routing**
5. **ipv6 cef**
6. **router ospfv3** *process-id*
7. **router-id** *ip-address*
8. **address-family ipv6 unicast**
9. **exit**
10. **exit**
11. **interface virtual-template** *number*
12. **ipv6 enable**
13. **no keepalive**
14. **exit**
15. **interface** *type number*
16. **ipv6 enable**
17. **ospfv3** *process-id* **area** *area-id* **ipv6** [**instance** *instance-id]*
18. **ospfv3** *process-id* **network manet**
19. **physical-interface** *type number*
20. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no virtual-template subinterface** **Example:** `Router(config)# no virtual-template subinterface`	Disables the virtual template on the subinterface.

	Command or Action	Purpose
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables IPv6 unicast routing.
Step 5	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables IPv6 Cisco Express Forwarding on the router.
Step 6	**router ospfv3** *process-id* **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 for IPv6 router configuration mode, and enters router configuration mode.
Step 7	**router-id** *ip-address* **Example:** `Router(config-router)# router-id 10.1.1.1`	Identifies a specific router rather than allowing the dynamic assignment of the router to occur.
Step 8	**address-family ipv6 unicast** **Example:** `Router(config-router)# address-family ipv6 unicast`	Specifies IPv6 unicast address prefixes and enters address family configuration mode.
Step 9	**exit** **Example:** `Router(config-router-af)# exit`	Returns to router configuration mode.
Step 10	**exit** **Example:** `Router(config-router)# exit`	Returns to global configuration mode.

Step 11	**interface virtual-template** *number*
	Example:
	`Router(config)#`
	`interface virtual-template 1`
		Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically to virtual access interfaces.

	Command or Action	Purpose
Step 12	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 processing on the virtual template.
Step 13	**no keepalive** **Example:** `Router(config-if)# no keepalive`	Turns off PPP keepalive messages.
Step 14	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 15	**interface** *type number* **Example:** `Router(config)# interface vmi 1`	Creates a VMI interface, and enters interface configuration mode.
Step 16	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 processing on the VMI interface that is not configured with an explicit IPv6 address.
Step 17	**ospfv3** *process-id* **area** *area-id* **ipv6** [**instance** *instance-id]* **Example:** `Router(config-if)# ospfv3 1 area 0 ipv6`	Attaches the interface to a specific OSPFv3 area and enables routing of IPv6 network traffic on this interface. • *process-id* --the value must match the ID configured with the **router ospfv3** global configuration command. • *instance-id* --automatically defaults to 0 for IPv6.
Step 18	**ospfv3** *process-id* **network manet** **Example:** `Router(config-if)# ospfv3 1 network manet`	Sets the network type to MANET.
Step 19	**physical-interface** *type number* **Example:** `Router(config-if)# physical-interface FastEthernet 0/1`	Creates the physical subinterface to be associated with the VMI interfaces on the router.

	Command or Action	Purpose
Step 20	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Fine-Tuning Radio-Aware Routing Link Metrics

Before You Begin

Complete the required task in the Configuring OSPFv3 in MANETs for Radio-Aware Routing, on page 198.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** *process-id* **cost dynamic hysteresis** [**threshold** *threshold-value* **]**
5. **ospfv3** *process-id* **cost dynamic weight throughput** *percent*
6. **ospfv3** *process-id* **cost dynamic weight resources** *percent*
7. **ospfv3** *process-id* **cost dynamic weight latency** *percent*
8. **ospfv3** *process-id* **cost dynamic weight L2-factor** *percent*
9. **ospfv3** *process-id* **area** *area-id* **ipv6** [**instance** *instance-id*]
10. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface vmi 1`	Creates a VMI interface, and enters interface configuration mode.
Step 4	**ospfv3** *process-id* **cost dynamic hysteresis** [**threshold** *threshold-value* **]** **Example:** `Router(config-if)# ospfv3 1 cost dynamic hysteresis threshold 1000`	Sets the hysteresis tolerance for the interface.
Step 5	**ospfv3** *process-id* **cost dynamic weight throughput** *percent* **Example:** `Router(config-if)# ospfv3 1 cost dynamic weight throughput 0`	Sets the metric for the throughput threshold.
Step 6	**ospfv3** *process-id* **cost dynamic weight resources** *percent* **Example:** `Router(config-if)# ospfv3 1 cost dynamic weight resources 29`	Sets the metric for the resource factor.
Step 7	**ospfv3** *process-id* **cost dynamic weight latency** *percent* **Example:** `Router(config-if)# ospfv3 1 cost dynamic weight latency 29`	Sets the threshold for the latency factor.
Step 8	**ospfv3** *process-id* **cost dynamic weight L2-factor** *percent* **Example:** `Router(config-if)# ospfv3 1 cost dynamic weight L2-factor 29`	Sets the metric for the Layer 2-to-Layer 3 delay factor.
Step 9	**ospfv3** *process-id* **area** *area-id* **ipv6** [**instance** *instance-id*] **Example:** `Router(config-if)# ospfv3 1 area 0 ipv6 instance 1`	Enables OSPF for IPv6 on an interface.
Step 10	**end** **Example:** `Router(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Enabling Selective Peering

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **address-family ipv6 unicast**
5. **exit**
6. **manet peering selective** [**redundancy** *redundancy-count*] [**per-interface]**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 for IPv6 router configuration mode, and enters router configuration mode.
Step 4	**address-family ipv6 unicast** **Example:** `Router(config-router)# address-family ipv6 unicast`	Specifies IPv6 unicast address prefixes.
Step 5	**exit** **Example:** `Router(config-router-af)# exit`	Returns to router configuration mode.

	Command or Action	Purpose
Step 6	**manet peering selective** [**redundancy** *redundancy-count*] [**per-interface]** **Example:** `Router(config-router)# manet peering selective`	Enables selective peering only for instances of the OSPF process for which the corresponding interface has been configured with the **ospfv3 network manet** command. • (Optional) **redundancy** *redundancy-count*--Changes the preferred number of redundant paths to any given peer. • (Optional) **per-interface**--Applies selective peering on a per-interface basis.
Step 7	**end** **Example:** `Router(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Preventing Full Peering with Neighbors with Poor Link Metrics

An RAR-compliant radio might not advertise link metrics to the router before a new OSPFv3 neighbor is discovered. You can configure OSPFv3 to wait for link metrics before considering a neighbor for OSPFv3 peering. You can specify a minimum metric threshold. If the radio-reported link metric is above this threshold, the neighbor will be held in two-way state. With this configuration, full peering with neighbors with poor link metrics can be effectively prevented.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** [*process-id*] **manet peering link-metrics** [*threshold*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vmi 1`	Creates a VMI interface, and enters interface configuration mode.
Step 4	**ospfv3** [*process-id*] **manet peering link-metrics** [*threshold*] **Example:** `Router(config-if)# ospfv3 manet peering link-metrics 200`	Configures an OSPFv3 process to wait for link metrics from a neighbor before attempting selective peering with that neighbor. • (Optional) *threshold*--Specifies that the link cost computed from the received link metrics from the radio must be below this value. Otherwise, the neighbor is held in a two-way state until metrics are received that result in a link cost below the configured level. The range is 0 to 65535.
Step 5	**end** **Example:** `Router(config-if)# end`	Optional) Returns to privileged EXEC mode.

Fine-Tuning Selective Peering with Link Metrics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** [*process-id*] **manet peering cost** {**threshold** *threshold-value* | **percent** *percent-value*}
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface vmi 1`	Creates a VMI interface, and enters interface configuration mode.
Step 4	**ospfv3** [*process-id*] **manet peering cost** {**threshold** *threshold-value* | **percent** *percent-value*} **Example:** `Router(config-if)# ospfv3 1 manet peering cost percent 10`	Sets a minimum cost change threshold necessary before a new neighbor is considered for selective peering. • Requires redundant paths to have an incrementally better path cost than the current best path cost specified either as an absolute value or as a percentage of the current best path cost.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Configuration Examples for OSPFv3 Extensions for MANETs

Example Configuring OSPFv3 in MANETs for Radio-Aware Routing

This example shows how to configure OSPFv3 in MANETs for use with RAR-compliant radios. For OSPFv3 to take advantage of radio feedback, OSPFv3 MANET is configured on the VMI.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service alignment detection
!
hostname Router1
!
boot-start-marker
boot-end-marker
```

```
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet 0/1
 no ip address
 shutdown
!
interface Ethernet 0/2
 no ip address
 shutdown
!
interface Ethernet 0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 1 network manet
 ospfv3 1 area 0 ipv6
 physical-interface FastEthernet 0/0
!
ip forward-protocol nd
!
router ospfv3 1
!
log-adjacency-changes
address-family ipv6 unicast
exit-address-family
!
control-plane
!
line con 0
 exec-timeout 0 0
 line aux 0
 line vty 0 4
 login
!
```

Example Fine-Tuning Radio-Aware Routing Link Metrics

This example shows the OSPFv3 extensions for MANET configuration with fine-tuning radio-aware routing link metrics:

```
!
version 15.2
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet 0/0
 no ip address
 pppoe enable group pppoe_group_1
!
interface Ethernet 0/1
 no ip address
 shutdown
!
interface Ethernet 0/2
 no ip address
 shutdown
!
interface Ethernet 0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 1 area 0 ipv6
 ospfv3 1 network manet
 ospfv3 1 cost dynamic hysteresis threshold 1000
 ospfv3 1 cost dynamic weight throughput 0
 ospfv3 1 cost dynamic weight latency 29
 ospfv3 1 cost dynamic weight L2-factor 29
 ospfv3 1 area 0 ipv6 instance 1
 physical-interface Ethernet 0/1
!
router ospfv3 1
 router-id 10.1.1.1
 timers throttle spf 1000 2000 2000
 !
 address-family ipv6 unicast
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
```

```
logging esm config
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Example Enabling Selective Peering

This example shows the OSPFv3 extensions for MANET configuration when selective peering is enabled:

```
!
version 15.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet 0/0
 no ip address
 pppoe enable group pppoe_group_1
!
interface Ethernet 0/1
 no ip address
 shutdown
!
interface Ethernet 0/2
 no ip address
 shutdown
!
interface Ethernet 0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
```

```
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 1 area 0 ipv6
 ospfv3 1 network manet
 ospfv3 1 cost dynamic hysteresis threshold 1000
 ospfv3 1 cost dynamic weight throughput 0
 ospfv3 1 cost dynamic weight latency 29
 ospfv3 1 cost dynamic weight L2-factor 29
 ospfv3 1 area 0 ipv6 instance 1
 physical-interface Ethernet 0/1
!
router ospfv3 1
 router-id 10.1.1.1
 manet peering selective
 timers throttle spf 1000 2000 2000
 !
 address-family ipv6 unicast
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging esm config
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Example Preventing Full Peering with Neighbors with Poor Link Metrics

This example shows the OSPFv3 extensions for MANET configuration to prevent full peering with neighbors with poor link metrics:

```
!
version 15.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
```

```
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet 0/0
 no ip address
 pppoe enable group pppoe_group_1
!
interface Ethernet 0/1
 no ip address
 shutdown
!
interface Ethernet 0/2
 no ip address
 shutdown
!
interface Ethernet 0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 1 area 0 ipv6
 ospfv3 1 network manet
 ospfv3 1 cost dynamic hysteresis threshold 1000
 ospfv3 1 cost dynamic weight throughput 0
 ospfv3 1 cost dynamic weight latency 29
 ospfv3 1 cost dynamic weight L2-factor 29
 ospfv3 1 manet peering link-metrics 200
 ospfv3 1 area 0 ipv6 instance 1
 physical-interface Ethernet 0/1
!
router ospfv3 1
 router-id 10.1.1.1
 manet peering selective
timers throttle spf 1000 2000 2000
 !
 address-family ipv6 unicast
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging esm config
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Example Fine-Tuning Selective Peering with Link Metrics

This example shows the OSPFv3 extensions for MANET configuration to fine-tune selective peering with link metrics:

```
!
version 15.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
subscriber authorization enable
!
subscriber profile pppoe_group_1
 pppoe service manet_radio
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
bba-group pppoe pppoe_group_1
 virtual-template 1
 service profile pppoe_group_1
!
interface Ethernet 0/0
 no ip address
 pppoe enable group pppoe_group_1
!
interface Ethernet 0/1
 no ip address
 shutdown
!
interface Ethernet 0/2
 no ip address
 shutdown
!
interface Ethernet 0/3
 no ip address
 shutdown
!
interface Virtual-Template1
 no ip address
 ipv6 enable
 no peer default ip address
 no keepalive
!
interface vmi1
 no ip address
 ipv6 enable
 ospfv3 1 area 0 ipv6
 ospfv3 1 network manet
 ospfv3 1 cost dynamic hysteresis threshold 1000
 ospfv3 1 cost dynamic weight throughput 0
 ospfv3 1 cost dynamic weight latency 29
 ospfv3 1 cost dynamic weight L2-factor 29
 ospfv3 1 manet peering cost percent 10
 ospfv3 1 manet peering link-metrics 200
 ospfv3 1 area 0 ipv6 instance 1
```

```
 physical-interface Ethernet 0/1
!
router ospfv3 1
 router-id 10.1.1.1
 manet peering selective
timers throttle spf 1000 2000 2000
 !
 address-family ipv6 unicast
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging esm config
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

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

Standards

Standard	Title
draft-chandra-ospf-manet-ext-02	*Extensions to OSPF to Support Mobile Ad Hoc Networking*

MIBs

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

RFCs

RFC	Title
RFC 5578	*PPP over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics*
RFC 5820	*Extensions to OSPF to Support Mobile Ad Hoc Networks*

Technical Assistance

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

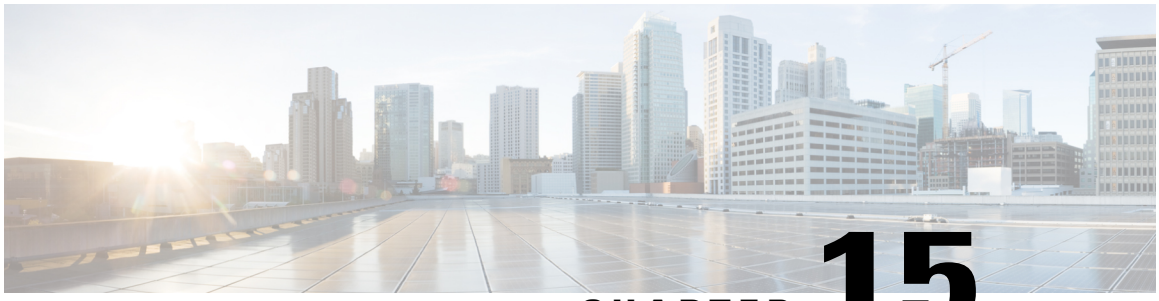
Feature Information for OSPFv3 Extensions for MANETs

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

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

Table 5: Feature Information for OSPFv3 Extensions for MANETs

Feature Name	Releases	Feature Information
OSPFv3 Extensions for MANETs	15.2(1)T	The OSPFv3 Extensions for MANETs feature optimizes OSPFv3 behavior for more efficient routing in highly mobile ad hoc environments. The following commands were introduced or modified: **manet cache**, **manet hello unicast**, **manet peering selective**, **manet willingness**, **ospfv3 manet peering cost**, **ospfv3 manet peering link-metrics**, **timers manet**, **timers throttle spf**.



CHAPTER 15

IP Multiplexing

You can use IP multiplexing to optimize IPv4 and IPv6 traffic in environments, such as a satellite network, where packet-per-second transmission limitations cause inefficient bandwidth utilization. IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

Finding Feature Information

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

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

Prerequisites for IP Multiplexing

You must configure an access list before IP multiplexing can work. Create an access control list (ACL) list by using the **ip access-list** or the **ipv6 access-list** command. When you configure an ACL to use with IP multiplexing, filter only traffic based on the destination address, destination port, and protocol type. If you configure an ACL with other filter characteristics, unexpected or undesirable multiplexing decisions might occur.

Information About IP Multiplexing

About IP Multiplexing

You can use IP multiplexing to optimize IPv4 and IPv6 traffic in environments, such as a satellite network, where packet-per-second transmission limitations cause inefficient bandwidth utilization. IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

Traffic Identification with Access Control Lists

IP multiplexing uses Cisco access control lists (ACLs) to identify outbound packets. IP multiplexing uses ACL definitions to identify traffic selected for multiplexing treatment. You can configure standard, extended, or named ACLs to define traffic you want to multiplex. Packets that are not identified by an ACL used for multiplexing are routed normally.

In general, an ACL statement for IP multiplexing should have this format:

permit udp any *host destination-IP-address UDP-port-number*

IP multiplexing makes caching decisions based on destination IP address, destination port, and protocol type. Although ACLs can be defined to filter packets based on other attributes, using other attributes in an IP multiplexing ACL can have unexpected and unwanted results.

IP multiplexing maintains the cache of recent ACL lookup results to optimize traffic classification.

For information about configuring an ACL, see the *Security Configuration Guide: Access Control Lists* publication.

Interface Types Supported with IP Multiplexing

These interface types support IP multiplexing:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IPv4 generic routing encapsulation (GRE) tunnel
- IPv6 GRE tunnel
- Ethernet, Fast Ethernet, and Gigabit Ethernet VLAN
- Virtual multipoint interface (VMI) over Ethernet, Fast Ethernet, and Gigabit Ethernet
- Virtual template on VMI

Both endpoints of the multiplex connection must be configured for multiplexing with corresponding source and destination addresses. If a superframe arrives at an interface with IP multiplexing not configured or not

configured to receive superframes from the destination device, the superframe is not demultiplexed, and the superframe is routed normally. If IP multiplexing is not configured, then outbound packets are routed normally.

IP Multiplexing Profiles

The attributes associated with an IP multiplexing connection between two devices are configured in an IP multiplexing profile.

Note You must configure an IP multiplexing profile for each endpoint of an IP multiplexing connection in the network.

You must define the following information for an IP multiplexing profile:

- Profile name
- ACL used to classify outbound IP packets as IP multiplexing traffic
- Source and destination IP addresses to be included in the superframe header
- Maximum amount of time the device waits to fill a superframe before sending a partial superframe

You can define the following optional information for an IP multiplexing profile:

- Maximum size of an outbound IP packet to be considered for multiplexing
- Maximum MTU size of a superframe
- Time-to-live (TTL) value to be included in the superframe IP header

IP Multiplexing Policies

An IP multiplexing policy is used to retain differentiated services code point (DSCP) priorities of the underlying data traffic. If you configure an IP multiplexing policy, you can configure DSCP values for the superframe header and specify that only the packets with a specified DSCP value be placed into the superframe. Note that a policy can match more than one DSCP value.

A device can have up to three multiplex policies for IPv6 and three multiplex policies for IPv4 defined on it. Multiplexing policies are global and apply to all multiplexing profiles on a device.

If the DSCP value assigned to a packet does not match any multiplexing policy, the device uses the default multiplexing policy for superframe multiplexing. Superframes for the default policy have a DSCP value set to 0.

If you do not configure an IP multiplexing policy, all IP multiplexing packets are sent using the default IP multiplexing policy with a DSCP value equal to 0.

The DSCP values in each packet header remains intact as the packet goes through the multiplexing and demultiplexing processes.

How to Configure IP Multiplexing

Configuring an IP Multiplexing Profile

You must configure an IP multiplexing profile for each endpoint of an IP multiplexing connection in the network.

When configuring IP multiplexing, you must configure each device before enabling the configuration. Failure to do so will result in lost packets at the end that is not yet configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux profile** *profile-name*
   - **ipv6 mux profile** *profile-name*
4. **access-list** {*standard-access-list-number* | *extended-access-list-number* | *name*}
5. **source** {*ip-addr* | *ipv6-addr* | **interface** *type*}
6. **destination** {*ip-addr* | *ipv6-addr*}
7. **holdtime** *milliseconds*
8. **maxlength** *bytes*
9. **mtu** *bytes*
10. **ttl** *hops*
11. **no singlepacket**
12. **no shutdown**
13. **end**
14. Enter one of the following commands:
    - **show ip mux profile** [*profile-name*]
    - **show ipv6 mux profile** [*profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux profile** *profile-name* • **ipv6 mux profile** *profile-name* **Example:** `Device(config)# ip mux profile routeRTP-SJ`	Creates an IP multiplexing profile with the specified name and enters IP multiplexing profile configuration mode.
Step 4	**access-list** {*standard-access-list-number* | *extended-access-list-number* | *name*} **Example:** `Device(config-ipmux-profile)# access-list routeRTP-SJ`	Applies the specified access list to the profile and uses the statements in the access list to identify outbound traffic for multiplexing. • *standard-access-list-number*—The range is 1 to 199. • *extended-access-list-number*—The range is 1300 to 2699. • *name*—Access list name to use with the IP multiplexing profile.
Step 5	**source** {*ip-addr* | *ipv6-addr* | **interface** *type*} **Example:** `Device(config-ipmux-profile)# source 192.0.2.1`	Designates the source IP address for the profile. • The source address is the IP address assigned to the outbound interface. • If you created an IPv4 profile, use an IPv4 address. If you created an IPv6 profile, use an IPv6 address. • If you use the **interface** keyword, IP multiplexing uses the IP address configured for that interface. Beware if you are using the **interface** keyword for an IPv6 interface with multiple IP addresses assigned to it. IP multiplexing might not use the IP address you want for multiplexing. • You must shut down the profile to change the source address. **Note** This source address must be configured as the destination address in the corresponding profile at the other end of the IP multiplexing connection.
Step 6	**destination** {*ip-addr* | *ipv6-addr*} **Example:** `Device(config-ipmux-profile)# destination 198.51.100.1`	Designates the IP address to which superframes will be sent from the particular profile. • The destination address must match the source address of the corresponding profile on the destination device. • If you created an IPv4 profile, use an IPv4 address. If you created an IPv6 profile, use an IPv6 address.

	Command or Action	Purpose
		• You must shut down the profile to change the destination address. **Note** This destination address must be configured as the source address in the corresponding profile at the other end of the IP multiplexing connection.
Step 7	**holdtime** *milliseconds* **Example:** `Device(config-ipmux-profile)# holdtime 150`	(Optional) Configures the amount of time in milliseconds (ms) that a multiplexing profile waits to fill the superframe before sending a partial superframe. • The range is 20 to 250 ms. • If you do not set a hold time, the profile uses 20 ms as a default.
Step 8	**maxlength** *bytes* **Example:** `Device(config-ipmux-profile)# maxlength 128`	(Optional) Configures the largest packet size that the multiplexing profile can hold for multiplexing. • A larger packet size will not be multiplexed even if it correctly matches the ACL attached to the profile. • The range is 64 to 1472 bytes. • If you do not configure a maximum packet length, any packet that fits into the superframe is multiplexed.
Step 9	**mtu** *bytes* **Example:** `Device(config-ipmux-profile)# mtu 1400`	(Optional) Configures the maximum size, in bytes, for the outbound superframe. • The range is 256 to 1500. • If you do not configure a MTU values, the profile uses 1500 bytes as a default. • The superframe size specified in the **mtu** command includes the IP and UDP headers for the superframe of 48 bytes for IPv6 and 28 bytes for IPv4 packets. Therefore an IPv6 MTU configured to 1400 bytes will accept 1352 bytes of data before sending a full superframe. An IPv4 MTU configured to 1400 bytes will accept 1372 bytes of data before sending a full superframe.
Step 10	**ttl** *hops* **Example:** `Device(config-ipmux-profile)# ttl 128`	(Optional) Configures the superframe time-to-live (TTL) for the IP header of the superframe. • The range is 1 to 255 hops. • By default, the TTL value is set to 64 hops.
Step 11	**no singlepacket** **Example:** `Device(config-ipmux-profile)# no singlepacket`	Configures the device to send the original packet unmodified if there is only one packet to multiplex when the hold timer expires. • By default, single packets are multiplexed into superframes when the hold timer expires.

	Command or Action	Purpose
Step 12	**no shutdown** **Example:** `Device(config-ipmux-profile)# no shutdown`	Activates the multiplexing profile. • If you want to change the ACL associated with the profile or the contents of the ACL, you must enter the **shutdown** command for the profile, make the changes and then enter the **no shutdown** command.
Step 13	**end** **Example:** `Device(config-ipmux-profile)# end`	Returns to privileged EXEC mode.
Step 14	Enter one of the following commands: • **show ip mux profile** [*profile-name*] • **show ipv6 mux profile** [*profile-name*] **Example:** `Device# show ip mux profile routeRTP-SJ`	Displays IP multiplexing statistics.

Configuring IP Multiplexing on an Interface

You must configure an interface for IP multiplexing. Once IP multiplexing is configured on an interface, all multiplex profiles are used to classify IP packets routed for transmission on the interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Enter one of the following commands:
   - **ip mux**
   - **ipv6 mux**
5. **end**
6. **show interface**
7. **show** {**ip** | **ipv6**} **mux interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/1`	Enters interface configuration mode for the specified interface.
Step 4	Enter one of the following commands: • **ip mux** • **ipv6 mux** **Example:** `Device(config-if)# ipv6 mux`	Enables IP multiplexing on the interface. • Use the **ip mux** command for an IPv4 interface. • Use the **ipv6 mux** command for an IPv6 interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show interface** **Example:** `Device# show interface`	Verifies that the interface is administratively up and whether the interface has an IPv4 or IPv6 address configured.
Step 7	**show** {**ip** | **ipv6**} **mux interface** **Example:** `Device# show ipv6 mux interface`	Displays IPv4 or IPv6 multiplexing statistics for the interface (depending on the command entered).

Configuring the UDP Port for Superframe Traffic

IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

The receiving device identifies incoming superframes by destination IP address, protocol type (UDP), and a UDP port number. A single UDP port number is used for all IP multiplexing traffic in the network.

Note If you do not configure a UDP port for IP multiplexing traffic, the system uses the default value of 6682. This value is inserted in the UDP header of the outbound superframe. If you use the default UDP port value, make sure that all devices sending or receiving IP multiplexing traffic use the same value.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux udpport** *port-number*
   - **ipv6 mux udpport** *port-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux udpport** *port-number* • **ipv6 mux udpport** *port-number* **Example:** `Device(config)# ip mux udpport 5000`	Specifies a destination UDP port to use for multiplexed packets. • The range is 1024 to 49151.

Configuring the IP Multiplexing Lookup Cache Size

The lookup cache maps the destination address, protocol type, and port number to a multiplexing profile to reduce performance overhead related to ACL lookups. You can configure the maximum size of the cache to manage memory utilization on the device.

The size of the IPv6 cache is 1,000,000 to 4,294,967,295 bytes, which corresponds to 10,419 to 44,739,242 entries.

The size of the IPv4 cache is 1,000,000 to 4,294,967,295 bytes which corresponds to 11,363 to 49,367,440 entries.

Note If you do not configure the cache size, the cache size defaults to 1,000,000 bytes, which will hold 11,363 entries for IPv4 multiplexing and 10,419 for IPv6 multiplexing.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mux cache** *size*
4. **end**
5. **show** {**ip** | **ipv6**} **mux cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip mux cache** *size* **Example:** `Device(config)# ip mux cache 5000000`	Configures the size of the IP multiplexing lookup cache. • The range is 1,000,000 to 4,294,967,295 bytes.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show** {**ip** | **ipv6**} **mux cache** **Example:** `Device# show ip mux cache`	Displays IPv4 or IPv6 multiplexing cache statistics (depending on the command entered).

Configuring the IP Multiplexing Policy with a DSCP Value for Outbound Superframes

Perform this task to create a multiplexing policy, specify the matching DSCP values for a superframe, and specify the outbound DSCP value for the header of the superframe.

If you do not configure a DSCP value for an outbound superframe, superframes are sent with a DSCP equal to 0.

If the DSCP value for packets selected for multiplexing does not match any of the **matchdscp** command values in the multiplexing policy, these packets are sent using the default multiplexing policy that has a DSCP set to 0.

A packet found to match the **matchdscp** command value is put in the superframe with the corresponding multiplexing policy.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux policy** *policy-name*
   - **ipv6 mux policy** *policy-name*
4. **outdscp** *DSCP-value*
5. **matchdscp** *DSCP-value*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux policy** *policy-name* • **ipv6 mux policy** *policy-name* **Example:** `Device(config)# ip mux policy RouteRTP-SJ`	Configures an IP policy with the specified name and enters either IP or IPv6 multiplexing policy configuration mode (depending on the command entered).
Step 4	**outdscp** *DSCP-value* **Example:** `Device(config-ipmux-policy)# outdscp 10`	Configures the DSCP value for the outbound superframe. • The range is 0 to 63. • For additional DSCP values that are valid, see the *IP Mobility Command Reference*.
Step 5	**matchdscp** *DSCP-value* **Example:** `Device(config-ipmux-policy)# matchdscp 45`	Configures the DSCP value that IP multiplexing uses to compare against the DSCP value in packets bound for multiplexing. • A match puts the packet in the superframe that corresponds to the IP multiplex policy. • You can enter more than one value. • The range is 0 to 63. • For additional DSCP values that are valid, see the *IP Mobility Command Reference*.
Step 6	**exit** **Example:** `Device(config-ipmux-policy)# exit`	Exits IP (or IPv6) multiplexing policy configuration mode.

Configuration Examples for IP Multiplexing

Example: Configuring an IP Multiplexing Profile

The following example shows an IPv4 multiplexing profile configuration:

```
ip mux profile r1a
  destination 10.1.1.1
  source 10.1.1.2
  access-list 199
  ttl 10
  holdtime 30
  mtu 1428
  maxlength 1400
```

Example: Configuring IP Multiplexing on an Interface

The following example show an IPv4 multiplexing configuration on an interface:

```
interface Ethernet 0/0
 ip mux
```

Examples: Configuring the UDP Port for Superframe Traffic

The following example shows a UDP port configuration for superframe traffic for IPv4:

```
ip mux udpport 12345
```

The following example shows a UDP port configuration for superframe traffic for IPv6:

```
ipv6 mux udpport 12345
```

Examples: Configuring the IP Multiplexing Lookup Cache Size

The following example shows an IPv4 multiplexing lookup cache size configuration:

```
ip mux cache 2000000
```

The following example shows an IPv6 multiplexing lookup cache size configuration:

```
ipv6 mux cache 2000000
```

Examples: Configuring the IP Multiplexing Policy With a DSCP Value for Outbound Superframes

The following example shows an IPv4 multiplexing policy:

```
ip mux policy dscp4
  matchdscp 4
  outdscp 4
```

The following example shows the IPv6 multiplexing policy:

```
ipv6 mux policy dscp4
  matchdscp 4
  outdscp 4
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP mobility commands	IP Mobility Command Reference

Technical Assistance

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

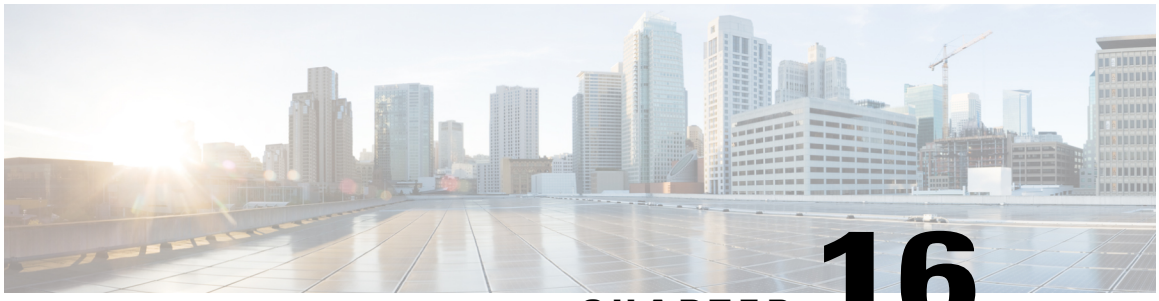
Feature Information for IP Multiplexing

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

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

Table 6: Feature Information for IP Multiplexing

Feature Name	Releases	Feature Information
IP Multiplexing	15.2(2)GC 15.2(4)M	IP multiplexing optimizes IPv4 and IPv6 traffic in environments, such as a satellite network, where packet-per-second transmission limitations cause inefficient bandwidth utilization. The following commands were introduced or modified: **access-list**, **destination**, **holdtime**, **ip mux**, **ip mux cache**, **ip mux policy**, **ip mux profile**, **ip mux udpport**, **ipv6 mux**, **ipv6 mux policy**, **ipv6 mux profile**, **ipv6 mux udpport**, **matchdscp**, **maxlength**, **mtu**, **outdscp**, **show mux**, **show mux cache**, **show mux interface**, **show mux profile**, **shutdown**, **singlepacket**, **source**, **ttl**.



CHAPTER 16

Restrictions for MANET Enhancements to PPPoE for Router-to-Radio Links

Virtual multipoint interfaces (VMIs) can be configured on routed ports on VLAN interfaces.

Information About MANET Enhancements to PPPoE for Router-to-Radio Links

About MANETs

Mobile Ad Hoc Networks (MANETs) for device-to-radio communications address the challenges faced when merging IP routing and mobile radio communications in ad hoc networking applications:

- Optimal route selection based on Layer 2 feedback from the radio network
- Faster convergence when nodes join and leave the network because devices are able to respond faster to network topology changes
- Efficient integration of point-to-point, directional radio topologies with multihop routing
- Flow-controlled communications between each radio and its partner device enables applications such as voice and video to work better because outages caused by moving links are reduced or eliminated. Sessions are more stable and remain active longer

Through the device-to-radio link, the radio can inform the device immediately when a node joins or leaves, and this enables the device to recognize topology changes more quickly than if it had to rely on timers. Without

this link-status notification from the radio, the device would likely time out while waiting for traffic. The link-status notification from the radio enables the device to respond faster to network topology changes. Metric information regarding the quality of a link is passed between the device and radio, enabling the device to more intelligently decide on which link to use.

With the link-status signaling provided by the device-to-radio link, applications such as voice and video work better because outages caused by topology changes are reduced or eliminated. Sessions are more stable and remain active longer.

Cross-layer feedback for device-to-radio integration of Radio-Aware Routing (RAR) takes advantage of the functions defined in RFC 5578. The RFC 5578 is an Internet Engineering Task Force (IETF) standard that defines PPP over Ethernet (PPPoE) extensions for Ethernet-based communications between a device and a mobile radio, that operates in a variable-bandwidth environment and has limited buffering capabilities. These extensions provide a PPPoE session-based mechanism for sharing radio network status such as link-quality metrics and establishing flow control between a device and an RAR-compliant radio.

An RAR-compliant radio initiates a Layer 2 PPPoE session with its adjacent device on behalf of every device and radio neighbor discovered in the network. These Layer 2 sessions are the means by which radio network status for each neighbor link is reported to the device. The radio establishes the correspondence between each PPPoE session and each link to a neighbor.

Routing Challenges for MANETs

Mobile Ad Hoc Networks (MANETs) enable users deployed in areas with no fixed communications infrastructure to access critical voice, video, and data services. For example, soldiers in the field can employ unified communications, multimedia applications, and real-time information dissemination to improve situational awareness and respond quickly to changing battlefield conditions. Disaster managers can use video conferences, database access, and collaborative tools to coordinate multiagency responses within an Incident Command System (ICS) framework. For event planners and trade show managers, MANETs represent a cost-effective way to accommodate mobile end users on a short-term basis.

In MANET environments, highly mobile nodes communicate with each other across bandwidth-constrained radio links. An individual node includes both a radio and a network device, with the two devices interconnected over an Ethernet. Because these nodes can rapidly join or leave the network, MANET routing topologies are highly dynamic. Fast convergence in a MANET becomes a challenge because the state of a node can change well before the event is detected by the normal timing mechanisms of the routing protocol.

Radio link quality in a MANET can vary dramatically because it can be affected by a variety of factors such as noise, fading, interference, and power fluctuation. As a result, avoiding congestion and determining optimal routing paths also pose significant challenges for the device network.

Directional radios that operate on a narrow beam tend to model the network as a series of physical point-to-point connections with neighbor nodes. This point-to-point model does not translate gracefully to multihop, multipoint device environments because it increases the size of each device's topology database and reduces routing efficiency.

Effective networking in a MANET environment therefore requires mechanisms by which

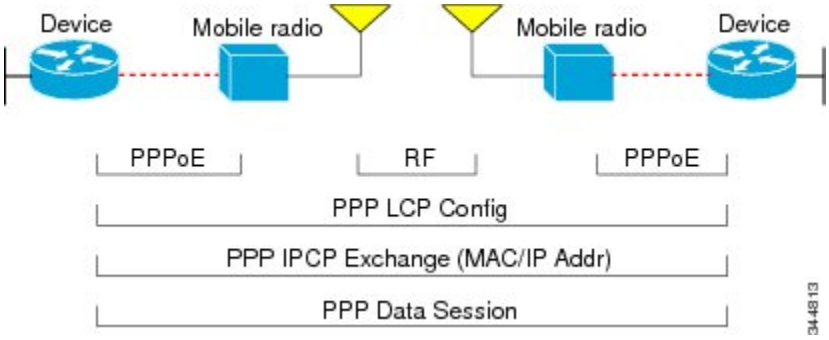
- Devices and radios can interoperate efficiently, and without impacting operation of the radio network.
- Radio point-to-point and device point-to-multipoint paradigms can be rationalized.
- Radios can report status to devices for each link and each neighbor.
- Devices can use this information to optimize routing decisions.

PPPoE Interfaces for Mobile Radio Communications

The Mobile Ad Hoc Network (MANET) implementation uses PPP over Ethernet (PPPoE) sessions to enable intranodal communications between a device and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (device-to-device). This is duplicated each time a radio establishes a new radio link. The virtual multipoint interface (VMI) on the device can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Underneath the VMI are virtual access interfaces that are associated with each of the PPP and PPPoE connections.

A PPPoE session is established between a device and a radio on behalf of every other device and radio neighbor located in the MANET. These Layer 2 sessions are the means by which radio network status gets reported to the Layer 3 processes in the device. The figure below shows the PPPoE session exchange between mobile devices and directional radios in a MANET network.

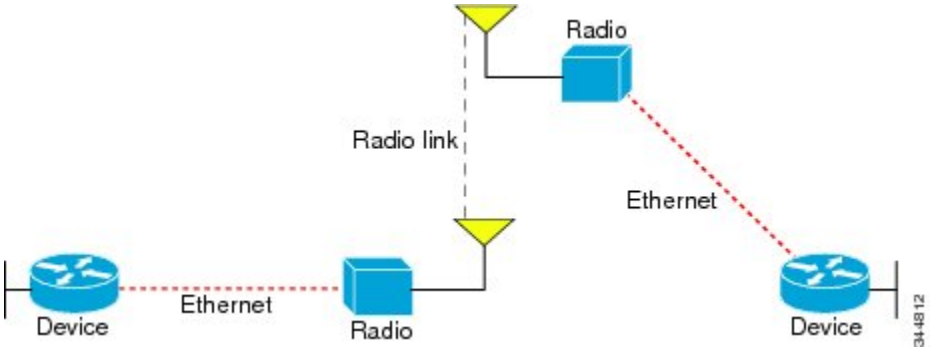
Figure 15: PPPoE Session Exchange Between Mobile Devices and Directional Radios



This capability requires that a Radio-Aware Routing (RAR)-compliant radio be connected to a device through Ethernet. The device always considers the Ethernet link to be up. If the radio side of the link goes down, the device waits until a routing update timeout occurs to declare the route down and then updates the routing table. The figure below shows a simple device-to-radio link topology.

The routing protocols optimized for VMI PPPoE are Enhanced Interior Gateway Routing Protocol (EIGRP) (IPv4, IPv6) and Open Shortest Path First version 3 (OSPFv3) for IPv4 and IPv6.

Figure 16: Device-to-Radio Link



Benefits of Virtual Multipoint Interfaces

The virtual multipoint interface (VMI) provides services that map outgoing packets to the appropriate PPP over Ethernet (PPPoE) sessions based on the next-hop forwarding address for that packet. The VMI also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through the VMI in aggregate mode, VMI replicates the packet and sends it through the virtual access interfaces to each of its neighbors.

Directional radios are frequently used in applications that require greater bandwidth, increased power-to-transmission range, or reduced probability of detection. These radios operate in a point-to-point mode and generally have no broadcast capability. However, the routing processes in Mobile Ad Hoc Networks (MANETs) operate most efficiently because the network link is treated as point-to-multipoint, with broadcast capability. For the device, modeling the MANET as a collection of point-to-point nodes has a dramatic impact on the size of its internal database.

The VMI within the device can aggregate all of the per-neighbor PPPoE sessions from the radio Ethernet connection. The VMI maps the sessions to appear to Layer 3 routing protocols and applications as a single point-to-multipoint, multiaccess, broadcast-capable network. However, the VMI preserves the integrity of the PPPoE sessions on the radio side so that each point-to-point connection can have its own quality of service (QoS) queue.

The VMI also relays the link-quality metric and neighbor up/down signaling from the radio to the routing protocols. The VMI signals are used by the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6 neighbors and the Open Shortest Path First version 3 (OSPFv3) for IPv6 neighbors.

IPv6 Address Support on VMIs

You can configure virtual multipoint interfaces (VMIs) with IPv6 addresses only, IPv4 addresses only, or both IPv4 and IPv6 addresses.

IPv6 addresses are assigned to individual device interfaces and enable the forwarding of IPv6 traffic globally on the device. By default, IPv6 addresses are not configured and IPv6 routing is disabled.

Note The *ipv6-address* argument in the **ipv6 address** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The */prefix-length* argument in the **ipv6 address** command is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) A slash mark must precede the decimal value.

Restrictions for IPv6 Addressing

The **ipv6 address** or the **ipv6 address eui-64** command can be used to configure multiple IPv6 global addresses within the same prefix on an interface. Multiple IPv6 link-local addresses on an interface are not supported.

OSPFv3 Address Families

The Open Shortest Path First version 3 9OSPFv3) address family feature is implemented according to RFC 5838 and enables the concurrent routing of IPv4 and IPv6 prefixes.

When this feature is enabled with Mobile Ad Hoc Networks (MANETs), IPv6 packets are routed in mobile environments over OSPFv3 using IPv4 or IPv6 addresses.

For configuration details, see the *IP Routing: OSPF Configuration Guide*.

Neighbor Up and Down Signaling for OSFPv3 and EIGRP

Mobile Ad Hoc Networks (MANETs) are highly dynamic environments. Nodes might move into, or out of, radio range at a fast pace. Each time a node joins or leaves, the network topology must be logically reconstructed by the devices. Routing protocols normally use timer-driven hello messages or neighbor timeouts to track topology changes, but MANETs reliance on these mechanisms can result in unacceptably slow convergence.

The neighbor up/down signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the device each time a link to another neighbor is established or terminated by the creation and termination of PPP over Ethernet (PPPoE) sessions. In the device, the routing protocols (Open Shortest Path First version 3 [OSPFv3] or Enhanced Interior Gateway Routing Protocol [EIGRP]) respond immediately to these signals by expediting formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the device immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high-speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When virtual multipoint interfaces (VMIs) with PPPoE are used and a partner node has left or a new one has joined, the radio informs the device immediately of the topology change. Upon receiving the signal, the device immediately declares the change and updates the routing tables. The signaling capability provides these advantages:

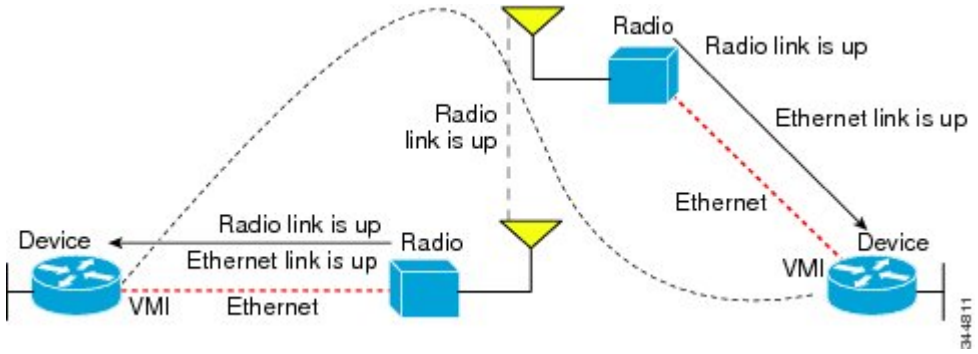
- Reduces routing delays and prevents applications from timing out
- Enables network-based applications and information to be delivered reliably and quickly over directional radio links
- Provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queueing and buffering
- Provides consistent quality of service for networks with multiple radios

The messaging allows for flexible rerouting when necessary because of these factors:

- Noise on the radio links
- Fading of the radio links
- Congestion of the radio links
- Radio link power fade
- Utilization of the radio

The figure below shows the signaling sequence that occurs when radio links go up and down.

Figure 17: Up and Down Signaling Sequence



PPPoE Credit-based and Metric-based Scaling and Flow Control

Each radio initiates a PPP over Ethernet (PPPoE) session with its local device as soon as the radio establishes a link to another radio. Once the PPPoE sessions are active for each node, a PPP session is then established end-to-end (device-to-device). This process is duplicated each time a radio establishes a new link.

The carrying capacity of each radio link might vary due to location changes or environmental conditions, and many radio transmission systems have limited buffering capabilities. To minimize the need for packet queueing in the radio, PPPoE protocol extensions enable the device to control traffic buffering in congestion situations. Implementing flow-control on these device-to-radio sessions allows use of quality of service (QoS) features such as fair queueing.

The flow-control solution utilizes a credit-granting mechanism documented in RFC 5578. When the PPPoE session is established, the radio can request a flow-controlled session. If the device acknowledges the request, all subsequent traffic must be flow controlled. If a flow-control session is requested and cannot be supported by the device, the session is terminated. Typically, both the radio and the device initially grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits are granted. Credits can be added incrementally over the course of a session.

Metrics scaling is used with high-performance radios that require high-speed links. The radio can express the maximum and current data rates with different scaler values. Credit scaling allows a radio to change the default credit grant (or scaling factor) of 64 bytes to its default value. You can display the maximum and current data rates and the scalar value set by the radio in the **show vmi neighbor detail** command output.

How to Configure MANET Enhancements to PPPoE for Router-to-Radio Links

Configuring a Subscriber Profile for PPPoE Service Selection

For virtual multipoint interfaces (VMIs) to work, you must configure a subscriber profile for PPP over Ethernet (PPPoE) service selection. In this task, you configure the PPPoE service name, which is used by Radio-Aware Routing (RAR)-compliant radio PPPoE clients to connect to the PPPoE server.

All PPPoE service names used for MANET implementations *must* begin with *manet_radio* for use with VMI and RFC 5578 features. Example service names are manet_radio and manet_radio_satellite.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **pppoe service manet_radio**
5. **exit**
6. **subscriber authorization enable**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**subscriber profile** *profile-name* **Example:** `Device(config)# subscriber profile manet`	Enters subscriber profile configuration mode.
Step 4	**pppoe service manet_radio** **Example:** `Device(config-sss-profile)# pppoe service manet_radio`	Adds a PPPoE MANET radio service name to a subscriber profile to enable the use of the VMI.
Step 5	**exit** **Example:** `Device(config-sss-profile)# exit`	Returns to global configuration mode.
Step 6	**subscriber authorization enable**	Enable Subscriber Service Switch type authorization.

	Command or Action	Purpose
	Example: `Device(config)# subscriber authorization enable`	• This command is required when virtual private dialup networks (VPDNs) are not used.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Assigning the Subscriber Profile to a PPPoE Profile

Perform this required task to assign a subscriber profile to a PPP over Ethernet (PPPoE) profile. In this configuration, the BBA group name should match the subscriber profile name previously defined in the subscriber profile. In this case, the profile name used as the service name is manet_radio.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**}	Defines a PPPoE profile and enters BBA group configuration mode.

	Command or Action	Purpose
	Example: `Device(config)# bba-group pppoe group1`	• The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Device(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Device(config-bba-group)# service profile subscriber-group1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. • Use the **refresh** *minutes* keyword and argument to cause the cached PPPoE configuration to time out after a specified number of minutes.
Step 6	**end** **Example:** `Device(config-bba-group)# end`	(Optional) Returns to privileged EXEC mode.

Troubleshooting Tips

Use the **show pppoe session** and the **debug pppoe** commands to troubleshoot PPP over Ethernet (PPPoE) sessions.

Enabling PPPoE Sessions on an Interface

Perform this required task to enable PPP over Ethernet (PPPoE) sessions on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pppoe enable** [**group** *group-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 3/1`	Specifies an interface and enters interface configuration mode. • Ethernet, Fast Ethernet, Gigabit Ethernet, VLANs, and VLAN subinterfaces can be used.
Step 4	**pppoe enable** [**group** *group-name*] **Example:** `Device(config-if)# pppoe enable group bba1`	Enables PPPoE sessions on an interface or subinterface.
Step 5	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Creating a Virtual Template for IPv4 and IPv6

Perform this optional task to create a virtual template for IPv4 and IPv6. You use the virtual template interface to dynamically clone configurations for each virtual access interface created for a virtual multipoint interface (VMI) neighbor.

Before You Begin

Cisco recommends that, when using the virtual template, you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy radio frequency (RF) link.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. Perform steps 5 and 8 if you are using IPv4. Perform steps 6, 7, and 8 if you are using IPv6. If you are using both, perform steps 5, 6, 7, and 8.
5. **ip unnumbered** *interface-type interface-number*
6. **ipv6 enable**
7. **ipv6 unnumbered** *interface-type interface-number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Creates a virtual template, and enters interface configuration mode.
Step 4	Perform steps 5 and 8 if you are using IPv4. Perform steps 6, 7, and 8 if you are using IPv6. If you are using both, perform steps 5, 6, 7, and 8. **Example:** **Example:**	--
Step 5	**ip unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on an interface without assigning an explicit IP address to the interface.

	Command or Action	Purpose
Step 6	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the interface.
Step 7	**ipv6 unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ipv6 unnumbered vmi I`	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
Step 8	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Creating a VMI for EIGRP IPv4

Perform this optional task to create the VMI for the Enhanced Interior Gateway Routing Protocol for IPv4 (EIGRP IPv4) and associate it with the interface on which PPP over Ethernet (PPPoE is enabled).

Before You Begin

When you create a virtual multipoint interface (VMI), assign the IPv4 address to that VMI definition.

The radio alerts the device with PADT messages that the Layer-2 radio frequency (RF) connection is no longer alive. Cisco recommends that you turn off the PPP keepalive messages to make CPU usage more efficient and to help avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

This configuration includes quality of service (QoS) fair queueing and a service policy applied to the VMI. Make certain that any fair queueing left over from any previous configurations is removed before applying the new policy map to the virtual template in the VMI configuration.

Note Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **no virtual-template subinterface**
5. **policy-map** *policy-mapname*
6. **class class-default**
7. **fair-queue**
8. **exit**
9. **exit**
10. **interface virtual-template** *number*
11. **ip unnumbered** *interface-type interface-number*
12. **service-policy output** *policy-mapname*
13. **no keepalive**
14. **interface** *type number*
15. **ip address** *address mask*
16. **no ip redirects**
17. **no ip split-horizon eigrp** *autonomous-system-number*
18. **physical-interface** *type number*
19. **exit**
20. **router eigrp** *autonomous-system-number*
21. **network** *network-number ip-mask*
22. **redistribute connected**
23. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip routing** **Example:** `Device(config)# ip routing`	Enables IP routing on the device.
Step 4	**no virtual-template subinterface** **Example:** `Device(config)# no virtual-template subinterface`	Disables the virtual template on the subinterface.
Step 5	**policy-map** *policy-mapname* **Example:** `Device(config)# policy-map fair-queue`	Enters QoS policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 6	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • Enters Qos policy-map class configuration mode.
Step 7	**fair-queue** **Example:** `Device(config-pmap-c)# fair-queue`	Enables weighted fair queueing (WFQ) on the interface.
Step 8	**exit** **Example:** `Device(config-pmap-c)# exit`	Returns to QoS policy-map configuration mode.
Step 9	**exit** **Example:** `Device(config-pmap)# exit`	Returns to global configuration mode.
Step 10	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

	Command or Action	Purpose
Step 11	**ip unnumbered** *interface-type interface-number* **Example:** `Device(config-if)# ip unnumbered vmi 1`	Enables IP processing of IPv4 on a serial interface without assigning an explicit IP address to the interface.
Step 12	**service-policy output** *policy-mapname* **Example:** `Device(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface, virtual circuit (VC), or to an output interface or VC. • The policy map is as the service policy for that interface or VC.
Step 13	**no keepalive** **Example:** no `Device(config-if)# no keepalive`	Turns off PPP keepalive messages to the interface.
Step 14	**interface** *type number* **Example:** `Device(config-if)# interface vmi 1`	Specifies the number of the VMI.
Step 15	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 16	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Disables the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco software is forced to resend a packet through the same interface on which it was received.
Step 17	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ip split-horizon eigrp 101`	Disables the split horizon mechanism for the specified session.
Step 18	**physical-interface** *type number* **Example:** `Device(config-if)# physical-interface FastEthernet 0/1`	Creates the physical subinterface to be associated with the VMIs on the device.

	Command or Action	Purpose
Step 19	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 20	**router eigrp** *autonomous-system-number* **Example:** `Device(config)# router eigrp 100`	Enables EIGRP routing on the device, identifies the autonomous system number, and enters router configuration mode.
Step 21	**network** *network-number ip-mask* **Example:** `Device(config-router)# network 209.165.200.225 255.255.255.224`	Identifies the EIGRP network.
Step 22	**redistribute connected** **Example:** `Device(config-router)# redistribute connected`	Redistributes routes from one routing domain into another routing domain.
Step 23	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Creating a VMI for EIGRP IPv6

Perform this optional task to create the VMI for the Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRP IPv6) and associate it with the interface on which PPP over Ethernet (PPPoE) is enabled.

Before You Begin

When you create a virtual multipoint interface (VMI), assign the IPv6 address to that VMI definition.

The radio alerts the device with PADT messages that the Layer-2 radio frequency (RF) connection is no longer alive. Cisco recommends that if you turn off the PPP keepalive messages to make CPU usage more efficient and help to avoid the potential for the device to terminate the connection if PPP keepalive packets are missed over a lossy RF link.

This configuration includes quality of service (QoS) fair queueing and a service policy applied to the VMI. Make certain that any fair queueing left over from any previous configurations is removed before applying the new policy map to the virtual template in the VMI configuration.

Note Do not assign any addresses to the corresponding physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no virtual-template subinterface**
4. **ipv6 unicast-routing**
5. **ipv6 cef**
6. **policy-map** *policy-mapname*
7. **class class-default**
8. **fair-queue**
9. **exit**
10. **exit**
11. **interface virtual-template** *number*
12. **ipv6 enable**
13. **no keepalive**
14. **service-policy output** *policy-mapname*
15. **interface** *type number*
16. **ipv6 address** *address*/*prefix-length*
17. **ipv6 enable**
18. **ipv6 eigrp** *as-number*
19. **no ipv6 redirects**
20. **no ipv6 split-horizon eigrp** *as-number*
21. **physical-interface** *type number*
22. **no shutdown**
23. **ipv6 router eigrp** *as-number*
24. **redistribute connected**
25. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no virtual-template subinterface** **Example:** `Device(config)# no virtual-template subinterface`	Disables the virtual template on the subinterface.
Step 4	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables IPv6 unicast routing.
Step 5	**ipv6 cef** **Example:** `Device(config)# ipv6 cef`	Enables IPv6 Cisco Express Forwarding on the device
Step 6	**policy-map** *policy-mapname* **Example:** `Device(config-pmap)# policy-map fair-queue`	Enters QoS policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 7	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • Enters QoS policy-map class configuration mode.
Step 8	**fair-queue** **Example:** `Device(config-pmap-c)# fair-queue`	Enables weighted fair queueing (WFQ) on the interface.
Step 9	**exit** **Example:** `Device(config-pmap-c)# exit`	Returns to QoS policy-map configuration mode.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Device(config-pmap)#  exit`	Returns to global configuration mode.
Step 11	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 12	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 routing on the virtual template.
Step 13	**no keepalive** **Example:** `Device(config-if)# no keepalive`	Turns off PPP keepalive messages to the virtual template.
Step 14	**service-policy output** *policy-mapname* **Example:** `Device(config-if)# service-policy output fair-queue`	Attaches a policy map to an input interface, virtual circuit (VC), or to an output interface or VC. • The policy map is as the service policy for that interface or VC.
Step 15	**interface** *type number* **Example:** `Device(config-if)# interface vmi 1`	Creates a VMI.
Step 16	**ipv6 address** *address*/*prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:0DB8::/32`	Specifies the IPv6 address for the interface.
Step 17	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 routing on the interface.

	Command or Action	Purpose
Step 18	**ipv6 eigrp** *as-number* **Example:** `Device(config-if)# ipv6 eigrp 1`	Enables the EIGRP for IPv6 on a specified interface and specifies the autonomous system number.
Step 19	**no ipv6 redirects** **Example:** `Device(config-if)# no ipv6 redirects`	Disables the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if the software is forced to resend a packet through the same interface on which the packet was received
Step 20	**no ipv6 split-horizon eigrp** *as-number* **Example:** `Device(config-if)# no ipv6 split-horizon eigrp 100`	Disables the split horizon for EIGRP IPv6. • Associates this command with a specific EIGRP autonomous system number.
Step 21	**physical-interface** *type number* **Example:** `Device(config-if)# physical-interface FastEthernet 1/0`	Creates the physical subinterface to be associated with the VMIs on the device.
Step 22	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface or prevents the interface from being shut down.
Step 23	**ipv6 router eigrp** *as-number* **Example:** `Device(config-if)# ipv6 router eigrp 100`	Places the device in router configuration mode, creates an EIGRP routing process in IPv6, and allows you to enter additional commands to configure this process.
Step 24	**redistribute connected** **Example:** `Device(config-router)# redistribute connected`	Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running. • Redistributes IPv6 routes from one routing domain into another routing domain.
Step 25	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Verifying the VMI Configuration

You can use the following commands to verify the virtual multipoint interface (VMI) configuration:

- **show pppoe session all**
- **show interface vmi**
- **show vmi neighbors**
- **show vmi neighbors detail**
- **show ip eigrp interfaces**
- **show ip eigrp neighbors**
- **show ipv6 eigrp interfaces**
- **show ipv6 eigrp neighbors**
- **show ipv6 ospf interface**

Configuration Examples for MANET Enhancements to PPPoE for Router-to-Radio Links

Example: Basic VMI PPPoE Configuration with EIGRP IPv4

The following example shows the basic virtual multipoint interface (VMI) PPP over Ethernet (PPPoE) configuration with the Enhanced Interior Gateway Routing Protocol for IPv4 (EIGRP IPv4) as the routing protocol. This configuration includes one VMI.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password test
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
```

```
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
```

```
 ip unnumbered vmi1
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.226 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
!
interface vmi1
 ip address 209.165.200.226 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 dampening-change 50
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Example: Basic VMI PPPoE Configuration with EIGRP IPv6

The following example shows the basic requirements for configuring a virtual multipoint interface (VMI) that uses the Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRP IPv6) as the routing protocol. It includes one VMI.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
ip cef
!
```

```
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
!
!
archive
 log config
!
!
policy-map FQ
 class class-default
  fair-queue
!
!
!
!
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
!
interface Loopback1
 ip address 209.165.200.226 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
```

```
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 physical-interface FastEthernet0/0
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
```

```
line aux 0
line vty 0 4
 login
!
end
```

Example: VMI PPPoE Configuration with EIGRP for IPv4 and IPv6

The following examples show how to configure the virtual multipoint interface (VMI) for PPP over Ethernet (PPPoE) using the Enhanced Interior Gateway Routing Protocol (EIGRP) as the IP routing protocol when you have both IPv4 and IPv6 addresses configured on the interface. This configuration includes one VMI. Though EIGRP allows you to use the same autonomous system (AS) number on an IPv4 EIGRP process and on an IPv6 process, we recommend using a unique AS number for each process for clarity.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
logging buffered 3000000
no logging console
enable password lab
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
subscriber profile test
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe test
 virtual-template 1
 service profile test
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
```

```
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 ipv6 enable
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
```

```
interface vmi1
 ip address 209.165.200.225 255.255.255.224
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 10
 dampening-interval 30
 physical-interface FastEthernet0/0
!
router eigrp 1
 redistribute connected
 network 209.165.200.225 255.255.255.224
 network 209.165.200.226 255.255.255.224
 auto-summary
!
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 router-id 10.9.1.1
 no shutdown
 redistribute connected
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Example: VMI Configuration Using Multiple Virtual Templates

The following example shows how to configure the virtual multipoint interface (VMI) by using multiple virtual templates. This example shows two VMIs, each with a different service name.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
!
subscriber profile router1_ground
```

```
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
policy-map FQ
 class class-default
  fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.225 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.225 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Example: PPPoE Configuration

In the following example, the subscriber profile uses a predefined string manet_radio to determine whether an inbound PPP over Ethernet (PPPoE) session is coming from a device that supports the virtual multipoint interface (VMI). All IP definitions are configured on the VMI rather than on the Fast Ethernet or virtual-template interfaces; when those interfaces are configured, do not specify either an IP address or an IPv6 address.

No IP address is specified, and IPv6 is enabled by default on the VMI:

```
subscriber profile list1
  pppoe service manet_radio
  subscriber authorization enable
!
bba-group pppoe bba1
  virtual-template 1
  service profile list1
!
interface FastEthernet0/1
  no ip address
  pppoe enable group bba1
!
interface Virtual-Template 1
  no ip address
  no peer default ip-address
!
interface vmi 1
  no ip address
  physical-interface FastEthernet0/1
```

Example: Configuring Two VMIs and Two Virtual Templates

The following example shows a configuration that includes two virtual multipoint interfaces (VMIs), two virtual templates, and two service names. You can configure multiple virtual template interfaces for your VMI PPP over Ethernet (PPPoE) connections. The selection of which virtual template to use is predicated on the service name sent by the radio during PPPoE session establishment.

In this example, any PPPoE request for a session (presentation of a PPPoE Active Discovery Initiate [PADI] packet) with the service name of “manet_radio_ground” uses Virtual-Template1 as the interface to be cloned. Conversely, any PADI presented by the radio with the service name of “manet_radio_satellite” uses Virtual-Template2.

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST -5
ip cef
no ip domain lookup
!
!
subscriber authorization enable
```

```
!
subscriber profile router1_ground
 pppoe service manet_radio_ground
!
subscriber profile router1_satellite
 pppoe service manet_radio_satellite
!
ipv6 unicast-routing
 policy-map FQ
 class class-default
 fair-queue
!
!
!
bba-group pppoe router1_ground
 virtual-template 1
 service profile router1_ground
!
bba-group pppoe router1_satellite
 virtual-template 2
 service profile router1_satellite
!
!
interface Ethernet0/0
 pppoe enable group router1_ground
!
interface Ethernet0/1
 pppoe enable group router1_satellite
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered vmi1
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface Virtual-Template2
 ip unnumbered vmi2
 load-interval 30
 no peer default ip address
 no keepalive
 service-policy output FQ
!
interface vmi1
 description ground connection
 ip address 209.165.200.226 255.255.255.224
 physical-interface Ethernet0/0
!
interface vmi2
 description satellite connection
 ip address 209.165.200.227 255.255.255.224
 physical-interface Ethernet0/1
!
router eigrp 1
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
PPPoE and virtual templates	*Dial Configuration Guide* Cisco IOS Dial Technologies Command Reference
PPPoE configuration and commands	*Broadband Access Aggregation and DSL Configuration Guide* Cisco IOS Broadband Access Aggregation and DSL Command Reference
IPv6 addressing and basic connectivity	*IPv6 Addressing and Basic Connectivity Configuration Guide* (part of the IPv6 Configuration Guide Library)
IPv6 commands	Cisco IOS IPv6 Command Reference
Open Shortest Path First version 3 (OSPFv3) address families	*IP Routing: OSPF Configuration Guide*

RFCs

RFC	Title
RFC 2373	*IP Version 6 Addressing Architecture*
RFC 2516	*A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 5578	*PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics*
RFC 5838	*Support of Address Families in OSPFv3*

Technical Assistance

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

Feature Information for MANET Enhancements to PPPoE for Router-to-Radio Links

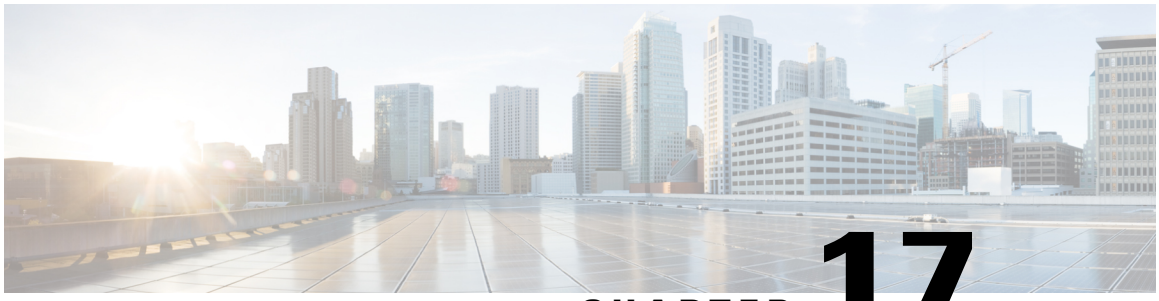
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

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

Table 7: Feature Information for MANET Enhancements to PPPoE for Router-to-Radio Links

Feature Name	Releases	Feature Information
MANET Enhancements to PPPoE for Router-to-Radio Links	12.4(15)XF 12.4(15)T 15.0(1)M	The MANET Enhancements to PPPoE for Router-to-Radio Links feature provides credit-based flow control and link-quality metrics over mobile radio links. Credit-based flow control provides in-band and out-of-band credit grants in each direction. Link-quality metrics report link performance statistics that are then used to influence routing. The following commands were introduced or modified: **show pppoe session**, **show vmi neighbors**.

Feature Name	Releases	Feature Information
Radio Aware Routing RFC 5578	15.1(3)T	Radio-Aware Routing incorporates RFC 5578 updates for interfacing Cisco devices to high-performance radios through PPP over Ethernet (PPPoE). The following commands were introduced or modified: **show vmi neighbors**.



CHAPTER 17

EIGRP Dynamic Metric Calculations

The EIGRP Dynamic Metric Calculations features enables the Enhanced Interior Gateway Routing Protocol (EIGRP) to use dynamic raw radio-link characteristics (current and maximum bandwidth, latency, and resources) to compute a composite EIGRP metric. A tunable hysteresis mechanism helps to avoid churn in the network as a result of the change in the link characteristics. In addition to the link characteristics, the L2/L3 API provides an indication when a new adjacency is discovered, or an existing unreachable adjacency is again reachable. When the Interior Gateway Routing Protocol (IGRP) receives the adjacency signals, it responds with an immediate Hello out the specified interface to expedite the discovery of the EIGRP peer.

Finding Feature Information

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

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

Prerequisites for EIGRP Dynamic Metric Calculations

Complete the virtual template and the appropriate PPP over Ethernet (PPPoE) configurations before performing this tasks in this module.

Information About EIGRP Dynamic Metric Calculations

Link-Quality Metrics Reporting for EIGRP

The quality of a radio link has a direct impact on the throughput that can be achieved by device-to-device traffic. The PPP over Ethernet (PPPoE) provides a process by which a device can request, or a radio can report, link-quality metric information. With the Cisco Enhanced Interior Gateway Routing Protocol (EIGRP) implementation, the route cost to a neighbor is dynamically updated based on metrics reported by the radio, thus allowing the best route to be chosen within a given set of radio links and reducing the effect of frequent routing changes.

The routing protocols receive raw radio-link data and compute a composite quality metric for each link In computing these metrics, you should consider these factors:

- Maximum data rate--the theoretical maximum data rate of the radio link, in scaled bits per second
- Current data rate--the current data rate achieved on the link, in scaled bits per second
- Resources--a percentage (0 to 100) that can represent the remaining amount of a resource (such as battery power)
- Latency--the transmission delay packets encounter, in milliseconds
- Relative link quality--a numeric value (0 to 100) representing relative quality, with 100 being the highest quality

You can weight metrics during the configuration process to emphasize or deemphasize particular characteristics. For example, if throughput is a particular concern, you can weight the *throughput* metric so that it is factored more heavily into the composite route cost. Similarly, a metric of no concern can be omitted from the composite calculation

Link metrics can change rapidly, often by very small degrees, which can result in a flood of meaningless routing updates. In a worst-case scenario, the network could churn almost continuously as it struggles to react to minor variations in link quality. To alleviate this concern, Cisco provides a tunable dampening mechanism that allows you to configure threshold values. Any metric change that falls below the threshold is ignored. The quality of a connection to a neighbor varies, based on various characteristics of the interface when EIGRP is used as the routing protocol. The routing protocol receives dynamic raw radio-link characteristics and computes a composite metric that is used to reduce the effect of frequent routing changes.

By using the tunable hysteresis mechanism, you can adjust the threshold to the routing changes that occur when the device receives a signal that a new peer has been discovered or that an existing peer is unreachable. The tunable metric is weighted and is adjusted dynamically to account for these characteristics:

- Current and maximum bandwidth
- Latency
- Resources
- Relative link quality (RLQ)

You can deconfigure individual weights, and you can clear all weights so that the cost returns to the default value for the interface type. Based on the routing changes that occur, you can determine the cost by applying these metrics.

EIGRP Cost Metrics for VMIs

When the Enhanced Interior Gateway Routing Protocol (EIGRP) is used as the routing protocol, metrics allow EIGRP to respond to routing changes. The link-state metric is advertised as the link cost in the device link advertisement. The reply sent to any routing query always contains the latest metric information. The exceptions that result in an immediate update being sent are:

- A down interface
- A down route
- Any change in a metric that results in the device selecting a new next hop

EIGRP receives dynamic raw radio-link characteristics and computes a composite EIGRP metric based on a proprietary formula. To avoid churn in the network as a result of the change in the link characteristics, EIGRP uses a tunable dampening mechanism.

EIGRP uses the metric weights along with a set of vector metrics to compute the composite metric for local routing information base (RIB) installation and route selections. The EIGRP composite metric is calculated using the formula:

metric = [K1 * BW + (K2 * BW) / (256 - Load) + K3 * Delay] * [K5 / (Reliability + K4)]

If K5 = 0, the formula reduces to metric = [K1 * BW + (K2 * BW)/(256 - Load) + K3 * Delay]

Note Use K values only after careful planning. Mismatched K values prevent a neighbor relationship from being built, which can cause your network to fail to converge.

The table below lists the EIGRP vector metrics and their descriptions.

Table 8: EIGRP Vector Metrics

Vector Metric	Description
BW	Minimum bandwidth of the route in kb/s. It can be 0 or any positive integer.
Delay	Route delay in tens of microseconds. It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
Reliability	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
Load	Effective load of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
MTU	Minimum maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

EIGRP monitors metric weights on an interface to allow for the tuning of EIGRP metric calculations and indicate the type of service (ToS). The table below lists the K-values and their default.

Table 9: EIGRP K-Value Defaults

Setting	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

Most configurations use the first two metrics—delay and bandwidth. The default formula of (BW + Delay) is the EIGRP metric. The bandwidth for the formula is scaled and inverted by this formula:

(10^7/minimum BW in kilobits per second)

You can change the weights, but these weights must be the same on all the devices.

For example, look at an EIGRP link where the bandwidth to a particular destination is 128k and the Relative Link Quality (RLQ) is 50 percent.

BW = (256 * 10000000) / 128 = 20000000

Delay = (((10000000000 / 128) * 100) / (50 * 1000)) * 256 = (40000000 / 10) = 4000000

Using the cut-down formula, the EIGRP metric calculation would simplify to 256*(BW + Delay), resulting in the following value:

Metric = (BW + Delay) = 20000000 + 4000000 = 240000000

VMI Metric to EIGRP Metric Conversion

The quality of connection to a virtual multipoint interface (VMI) neighbor varies based on various characteristics computed dynamically based on the feedback from Layer 2 to Layer 3. The table below lists the Enhanced Interior Gateway Routing Protocol (EIGRP) metrics and their significance.

Table 10: EIGRP MANET Metrics for VMI Interfaces

Metric		Significance
Current data rate	uint64_t	The current data rate reported from the radio. EIGRP converts the value into kilobits per second.

Metric		Significance
Max data rate	uint64_t	The maximum data rate reported from the radio. EIGRP converts the value into kilobits per second.
Latency	unsigned int	The latency computed and reported by the radio in milliseconds.
Resources	unsigned int	The resources computed by the radio. A representation of resources, such as battery power, ranges from 0 to 100. If a radio does not report dynamic resources, the value is always 100.
Relative link quality	unsigned int	An opaque number that ranges from 0 to 100 is computed by the radio, representing radio's view of link quality. 0 represents the worst possible link, 100 represents the best possible link.
Link-load	unsigned int	An opaque number that ranges from 0 to 100 is computed by VMI, representing the load on the Ethernet link. 0 represents an idle Ethernet link, 100 represents a fully loaded Ethernet link. Note that this is not associated with the radio link.

The table below shows how these EIGRP vector metric values map to the basic EIGRP interface parameters.

Table 11: Mapping of VMI Metric Values to EIGRP Vector Metrics Values

VMI Metric	EIGRP Metric	Mapping
Current data rate	Bandwidth	Calculated: bandwidth = (256 * 10000000) / (current data rate / 1000)
Relative link quality resources	Reliability	Calculated: reliability = (255 * (relative link quality) / 100)) * (resources / 100)

VMI Metric	EIGRP Metric	Mapping
Current data rate Relative link quality	Delay	Calculated: delay = 256 * (1E10 / (current data rate / 1000)) * ((100 / relative link quality) / 1000) / 10
Load	Load	Calculated: load = ((255 * link-load) / 100)

EIGRP Metric Dampening for VMIs

Rapid changes in metric components can affect the network by requiring that prefixes learned though the virtual multipoint interface (VMI) be updated and sent to all adjacencies. This update can result in further updates and, in a worst-case scenario, cause network-wide churn. To prevent such effects, metrics can be dampened, or thresholds set, so that any change that does not exceed the dampening threshold is ignored.

Network changes that cause an immediate update include

- A down interface
- A down route
- Any change in a metric that results in the device selecting a new next hop

Dampening the metric changes can be configured based on change or time intervals.

If the dampening method is change-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, are not advertised to adjacencies until the computed metric changes from the last advertised value significantly enough to cause an update to be sent.

If this dampening method is interval-based, changes in routes learned though a specific interface, or in the metrics for a specific interface, are not advertised to adjacencies until the specified interval is met, unless the change results in a new route path selection.

When the timer expires, any routes that have outstanding changes to report are sent. If a route changes, such that the final metric of the route matches the last updated metric, no update is sent.

How to Configure EIGRP Dynamic Metric Calculations

Setting the EIGRP Change-based Dampening Interval Using Classic-Style Configuration

Perform this optional task to set the Enhanced Interior Gateway Routing Protocol (EIGRP) change-based dampening interval for virtual multipoint interfaces (VMIs) using classic-style configuration. Configuring the **router eigrp** *autonomous-system-number* command creates an EIGRP configuration referred to as autonomous system (AS) configuration. An EIGRP AS configuration creates an EIGRP routing instance that can be used for tagging routing information.

You can configure this feature with either an IPv4 or an IPv6 address, or you can use both. If you are using both IPv4 and IPv6, complete the entire configuration.

This configuration sets the threshold to 50 percent tolerance for routing updates involving VMIs and peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **no ip redirects**
6. **no ip split-horizon eigrp** *autonomous-system-number*
7. **ip dampening-change eigrp** *autonomous-system-number percentage*
8. Enter one of the following commands:
   - **ipv6 address** *address*
   - **ipv6 enable**
9. **ipv6 eigrp** *autonomous-system-number*
10. **no ipv6 split-horizon eigrp** *autonomous-system-number*
11. **ipv6 dampening-change eigrp** *autonomous-system-number percentage*
12. **router eigrp** *autonomous-system-number*
13. **network** *address*
14. **ipv6 router eigrp** *autonomous-system-number*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vmi 1`	Enters interface configuration mode and creates a VMI.

	Command or Action	Purpose
Step 4	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 5	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Prevents the device from sending redirects.
Step 6	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ip split-horizon eigrp 101`	Disables the EIGRP split horizon.
Step 7	**ip dampening-change eigrp** *autonomous-system-number percentage* **Example:** `Device(config-if)# ip dampening-change eigrp 1 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes for IPv4.

Step 8	Enter one of the following commands:
	• **ipv6 address** *address*
	• **ipv6 enable**
	Example:
	`Device(config-if)# ipv6 address 2001:0DB8::/32`
	Example:
	`Device(config-if)# ipv6 enable`
		Specifies the IPv6 address.
		or
		Enables IPv6 routing on the interface.

Step 9	**ipv6 eigrp** *autonomous-system-number* **Example:** `Device(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on the interface.
Step 10	**no ipv6 split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ipv6 split-horizon eigrp 1`	Disables the sending of IPv6 redirect messages on an interface.

	Command or Action	Purpose
Step 11	**ipv6 dampening-change eigrp** *autonomous-system-number percentage* **Example:** `Device(config-if)# ipv6 dampening-change eigrp 1 30`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes for IPv6.
Step 12	**router eigrp** *autonomous-system-number* **Example:** `Device(config-if)# router eigrp 1`	Configures the EIGRP address family process and enters router configuration mode.
Step 13	**network** *address* **Example:** `Device(config-router)# network 209.165.200.225`	Configures the network address.
Step 14	**ipv6 router eigrp** *autonomous-system-number* **Example:** `Device(config-router)# ipv6 router eigrp 1`	Configures an EIGRP routing process in IPv6.
Step 15	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Setting the EIGRP Change-based Dampening Interval Using Named-Style Configuration

Perform this optional task to set the Enhanced Interior Gateway Routing Protocol (EIGRP) change-based dampening interval for virtual multipoint interfaces (VMIs) using named-style configuration. Configuring the **router eigrp** *virtual-instance-name* command creates an EIGRP configuration referred to as an EIGRP named configuration. An EIGRP named configuration does not create an EIGRP routing instance by itself. EIGRP named configuration is a base configuration that is required to define address-family configurations under it that are used for routing.

You can configure this feature with either an IPv4 or an IPv6 address, or you can use both. If you are using both IPv4 and IPv6, then complete the entire configuration.

This configuration sets the threshold to 50 percent tolerance for routing updates involving VMIs and peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **no ip redirects**
6. Enter one of the following commands:
   - **ipv6 address** *address*
   - **ipv6 enable**
7. **router eigrp** *virtual-instance-name*
8. **address-family ipv4 autonomous-system** *autonomous-system-number*
9. **network** *address*
10. **af-interface** *type number*
11. **dampening-change** *percentage*
12. **exit**
13. **exit**
14. **address-family ipv6 autonomous-system** *autonomous-system-number*
15. **af-interface** *type number*
16. **dampening-change** *percentage*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vmi 1`	Enters interface configuration mode and creates a VMI.

	Command or Action	Purpose
Step 4	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 5	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Prevents the device from sending redirects.

Step 6	Enter one of the following commands:
	• **ipv6 address** *address*
	• **ipv6 enable**
	Example:
	`Device(config-if)# ipv6 address 2001:0DB8::/32`
	Example:
	`Device(config-if)# ipv6 enable`
		Specifies the IPv6 address.
		or
		Enables IPv6 routing on the interface.

Step 7	**router eigrp** *virtual-instance-name* **Example:** `Device(config-if)# router eigrp name`	Enables EIGRP for IPv6 on the interface, and enters router configuration mode.
Step 8	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP routing instance.
Step 9	**network** *address* **Example:** `Device(config-router-af)# network 209.165.200.225`	Configures the network address.
Step 10	**af-interface** *type number* **Example:** `Device(config-router-af)# af-interface vmi 1`	Enters address family interface configuration mode.

	Command or Action	Purpose
Step 11	**dampening-change** *percentage* **Example:** `Device(config-router-af-interface)# dampening-change 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family.
Step 12	**exit** **Example:** `Device(config-router-af-interface)# exit`	Exits address-family interface configuration mode.
Step 13	**exit** **Example:** `Device(config-router-af)# exit`	Exits address-family configuration mode and enters router configuration mode.
Step 14	**address-family ipv6 autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP routing instance for IPv6.
Step 15	**af-interface** *type number* **Example:** `Device(config-router-af)# af-interface vmi 1`	Enters address family interface configuration mode.
Step 16	**dampening-change** *percentage* **Example:** `Device(config-router-af-interface)# dampening-change 50`	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface.
Step 17	**end** **Example:** `Device(config-router-af-interface)# end`	(Optional) Returns to privileged EXEC mode.

Setting the EIGRP Interval-based Dampening Interval Using Classic-Style Configuration

Perform this optional task to set an Enhanced Interior Gateway Routing Protocol (EIGRP) interval-based dampening interval for virtual multipoint interfaces (VMIs) using classic-style configuration. Configuring the **router eigrp** *autonomous-system-number* command creates an EIGRP configuration referred to as autonomous system (AS) configuration. An EIGRP AS configuration creates an EIGRP routing instance that can be used for tagging routing information.

This configuration sets the interval to 30 seconds at which updates occur for topology changes that affect VMIs and peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **no ip redirects**
6. **no ip split-horizon eigrp** *autonomous-system-number*
7. **ip dampening-interval eigrp** *autonomous-system-number interval*
8. Enter one of the following commands:
   - **ipv6 address** *address*
   - **ipv6 enable**
9. **ipv6 eigrp** *autonomous-system-number*
10. **no ipv6 split-horizon eigrp** *autonomous-system-number*
11. **ipv6 dampening-interval eigrp** *autonomous-system-number interval*
12. **router eigrp** *autonomous-system-number*
13. **network** *address*
14. **ipv6 router eigrp** *autonomous-system-number*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vmi 1`	Enters interface configuration mode and creates a VMI.
Step 4	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 5	**no ip redirects** **Example:** `Device(config-if)# no ip redirect`	Prevents the device from sending redirects.
Step 6	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ip split-horizon eigrp 101`	Disables the EIGRP split horizon.
Step 7	**ip dampening-interval eigrp** *autonomous-system-number interval* **Example:** `Device(config-if)# ip dampening-change eigrp 1 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.

Step 8	Enter one of the following commands:
	• **ipv6 address** *address*
	• **ipv6 enable**
	
	Example:
	`Device(config-if)# ipv6 address 2001:0DB8::/32`
	
	Example:
	`Device(config-if)# ipv6 enable`
		Specifies the IPv6 address.
		or
		Enables IPv6 routing on the interface.

	Command or Action	Purpose
Step 9	**ipv6 eigrp** *autonomous-system-number* **Example:** `Device(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on the interface.
Step 10	**no ipv6 split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ipv6 split-horizon eigrp 1`	Disables the sending of IPv6 redirect messages on an interface.
Step 11	**ipv6 dampening-interval eigrp** *autonomous-system-number interval* **Example:** `Device(config-if)# ipv6 dampening-interval eigrp 1 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 12	**router eigrp** *autonomous-system-number* **Example:** `Device(config-if)# router eigrp 1`	Configures the EIGRP address family process and enters router configuration mode.
Step 13	**network** *address* **Example:** `Device(config-router)# network 209.165.200.225`	Configures the network address.
Step 14	**ipv6 router eigrp** *autonomous-system-number* **Example:** `Device(config-router)# ipv6 router eigrp 1`	Configures an EIGRP routing process in IPv6.
Step 15	**end** **Example:** `Device(config-router)# end`	(Optional) Returns to privileged EXEC mode.

Setting the EIGRP Interval-based Dampening Interval Using Named-Style Configuration

Perform this optional task to set an Enhanced Interior Gateway Routing Protocol (EIGRP) interval-based dampening interval for virtual multipoint interfaces (VMIs) using named-style configuration. Configuring the **router eigrp eigrp** *virtual-instance-name* command creates an EIGRP configuration referred to as an EIGRP named configuration. An EIGRP named configuration does not create an EIGRP routing instance by itself. EIGRP named configuration is a base configuration that is required to define address-family configurations under it that are used for routing.

This configuration sets the interval to 30 seconds at which updates occur for topology changes that affect VMIs and peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **no ip redirects**
6. Enter one of the following commands:
   - **ipv6 address** *address*
   - **ipv6 enable**
7. **router eigrp** *virtual-instance-name*
8. **address-family ipv4 autonomous-system** *autonomous-system-number*
9. **network** *address*
10. **af-interface** *type number*
11. **dampening-interval** *interval*
12. **exit**
13. **exit**
14. **address-family ipv6 autonomous-system** *autonomous-system-number*
15. **af-interface** *type number*
16. **dampening-interval** *interval*
17. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface vmi 1`	Enters interface configuration mode and creates a VMI.
Step 4	**ip address** *address mask* **Example:** `Device(config-if)# ip address 209.165.200.225 255.255.255.224`	Specifies the IP address of the VMI.
Step 5	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Prevents the device from sending redirects.

Step 6	Enter one of the following commands:
	• **ipv6 address** *address*
	• **ipv6 enable**
	Example:
	`Device(config-if)# ipv6 address 2001:0DB8::/32`
	Example:
	`Device(config-if)# ipv6 enable`
		Specifies the IPv6 address.
		or
		Enables IPv6 routing on the interface.

Step 7	**router eigrp** *virtual-instance-name* **Example:** `device(config-if)# router eigrp name`	Enables EIGRP for IPv6 on the interface, and enters router configuration mode.

	Command or Action	Purpose
Step 8	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `device(config-router)# address-family ipv4 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP routing instance.
Step 9	**network** *address* **Example:** `device(config-router-af)# network 209.165.200.225`	Configures the network address.
Step 10	**af-interface** *type number* **Example:** `device(config-router-af)# af-interface vmi 1`	Enters address family interface configuration mode.
Step 11	**dampening-interval** *interval* **Example:** `device(config-router-af-interface)# dampening-interval 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 12	**exit** **Example:** `device(config-router-af-interface)# exit`	Exits address family interface configuration mode.
Step 13	**exit** **Example:** `device(config-router-af)# exit`	Exits address family configuration mode and enters the router configuration mode.
Step 14	**address-family ipv6 autonomous-system** *autonomous-system-number* **Example:** `device(config-router)# address-family ipv6 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP routing instance for IPv6.
Step 15	**af-interface** *type number* **Example:** `device(config-router-af)# af-interface vmi 1`	Enters address family interface configuration mode.

	Command or Action	Purpose
Step 16	**dampening-interval** *interval* **Example:** `device(config-router-af-interface)# dampening-interval 30`	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface.
Step 17	**end** **Example:** `device(config-router-af-interface)# end`	(Optional) Returns to privileged EXEC mode.

Configuration Examples for EIGRP Dynamic Metric Calculations

Example: EIGRP Change-based Dampening for VMIs

The following example configures the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 5400
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# dampening-interval 45
```

Example: EIGRP Interval-based Dampening for VMIs

The following example configures the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 5400
Device(config-router-af)# af-interface ethernet 0/0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Enhanced Interior Gateway Routing Protocol (EIGRP) configuration tasks and commands	*IP Routing: EIGRP Configuration Guide* Cisco IOS IP Routing: EIGRP Command Reference
IPv6 configuration tasks and commands	*IPv6 Configuration Library* Cisco IOS IPv6 Command Reference

Technical Assistance

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

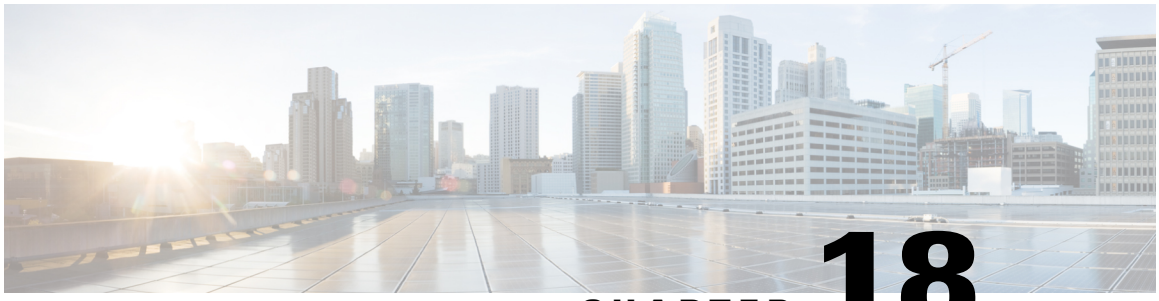
Feature Information for EIGRP Dynamic Metric Calculations

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

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

Table 12: Feature Information for EIGRP Dynamic Metric Calculations

Feature Name	Releases	Feature Information
EIGRP Dynamic Metric Calculations	12.4(15)XF 12.4(15)T 15.0(1)M	The EIGRP Dynamic Metric Calculations features enables the Enhanced Interior Gateway Routing Protocol (EIGRP) to use dynamic raw radio-link characteristics (current and maximum bandwidth, latency, and resources) to compute a composite EIGRP metric. A tunable hysteresis mechanism helps to avoid churn in the network as a result of the change in the link characteristics. In addition to the link characteristics, the L2/L3 API provides an indication when a new adjacency is discovered, or an existing unreachable adjacency is again reachable. When the Interior Gateway Routing Protocol (IGRP) receives the adjacency signals, it responds with an immediate Hello out the specified interface to expedite the discovery of the EIGRP peer. The following commands were introduced or modified: **dampening-change**, **dampening-interval**, **debug eigrp notifications**, **debug vmi**.



CHAPTER 18

Multicast for Virtual Multipoint Interfaces

The Multicast for Virtual Multipoint Interfaces feature enables multicast support for RFC 5578-compliant Radio-Aware Routing (RAR). Multicast is defined as a network group membership spanning the entire network. The virtual multipoint interface (VMI) operates in aggregate mode, which means that all virtual access interfaces created by PPP over Ethernet (PPPoE) sessions are aggregated logically under the configured VMI. Packets sent to the VMI are forwarded to the correct virtual access interface. When a VMI operates in aggregate mode, the interfaces operate in nonbroadcast multiple access (NBMA) mode. Multicast traffic is forwarded only the he NBMA neighbors where a listener for that group is present.

Finding Feature Information

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

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

Restrictions for Multicast for Virtual Multipoint Interfaces

Only IPv4 is supported for nonbroadcast multiple access (NBMA) multicasting.

Information About Multicast for Virtual Multipoint Interfaces

Multicast Support for VMIs

By default, virtual multipoint interfaces (VMIs) operate in aggregate mode, which means that all of the virtual access interfaces created by PPP over Ethernet (PPPoE) sessions are aggregated logically under the configured VMI. Applications above Layer 2, such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First version 3 (OSPFv3), should be defined only on the VMI. Packets sent to the VMI are forwarded to the correct virtual access interface. When VMIs are in aggregate mode, they operate in nonbroadcast multiple access (NBMA) mode. Multicast traffic is forwarded only to the NBMA neighbors where a listener for that group is present.

If you are running multicast applications that require the virtual access interfaces to be exposed to applications above Layer 2 directly, you can configure the VMI to operate in bypass mode. Most multicast applications require that the virtual access interfaces be exposed directly to the routing protocols to ensure that the multicast Reverse Path Forwarding (RPF) can operate as expected. When you use the bypass mode, you must define a VMI to handle presentation of cross-layer signals such as, neighbor up, neighbor down, and metrics. Applications are aware of the actual underlying virtual access interfaces and send packets to them directly. Additional information is required on the virtual template configuration.

Multicast Routing in NBMA Mode

Multicast is defined as a network group membership spanning the entire network. Usually, multicast is unidirectional from a source to a group of receivers. In both IPv4 and IPv6 architectures, a portion of the address space is reserved for multicast groups, and group addresses are requested to and assigned by Internet Assigned Numbers Authority (IANA). See the table below for IPv4 examples.

Table 13: Assigned IPv4 Multicast Addresses

Addresses	Usage
224.0.0.1	All hosts
224.0.0.2	All multicast hosts
224.0.0.5	Open Shortest Path First (OSPF) devices
224.0.0.10	Interior Gateway Routing Protocol (IGRP) devices
224.0.0.13	All Protocol Independent Multicast (PIM) devices
224.0.0.19 to 224.0.0.255	Unassigned

Nonbroadcast multiple access (NBMA) mode is achieved on a virtual multipoint interface (VMI) in aggregate mode. When operating in multicast NBMA mode, only the virtual interfaces that are part of the multicast tree receive multicast traffic.

How to Configure Multicast for Virtual Multipoint Interfaces

Enabling Bypass Mode for Multicast Applications

Perform this optional task to enable bypass mode on a VMI and override the default aggregation that occurs on VMIs. Bypass mode is recommended for multicast applications.

Before You Begin

Configure the virtual template and the appropriate PPP over Ethernet (PPPoE) sessions for the virtual multipoint interface (VMI) before performing this task.

Note Using bypass mode can cause databases in the applications to be larger because knowledge of more interfaces is required for normal operation.
After you enter the **mode bypass** command, Cisco recommends that you copy the running configuration to NVRAM because the default mode of operation for VMI is to logically aggregate the virtual access interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vmi** *interface-number*
4. **physical-interface** *type number*
5. **mode bypass**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface vmi** *interface-number* **Example:** `Device(config)# interface vmi 1`	Enters interface configuration mode and creates a VMI.
Step 4	**physical-interface** *type number* **Example:** `Device(config-if)# physical-interface fa 0/0`	Creates the physical subinterface to be associated with VMI on the device.
Step 5	**mode bypass** **Example:** `Device(config-if)# mode bypass`	Overrides the default aggregation on the VMI and sets the mode to bypass to support multicast traffic on the interface.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Multicast for Virtual Multipoint Interfaces

Examples: IP Address Coordination for the VMI in Aggregate Mode

The default mode for operation of the virtual multipoint interface (VMI) is aggregate mode. In aggregate mode, all of the virtual access interfaces created by PPP over Ethernet (PPPoE) sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First version 3 (OSPFv3), should be defined on the VMI only. Packets sent to the VMI will be correctly forwarded to the correct virtual access interface.

The next examples show the IP address coordination needed between the virtual-template configuration and the VMI configuration.

The following example shows the configuration of VMI in aggregate mode using IPv4 as the routing protocol:

```
!
interface Virtual-Template1
 ip unnumbered vmi1
 service-policy output FQ
!
interface vmi1
 ip address 2.2.2.1 255.255.255.0
```

```
 physical-interface FastEthernet 0/0
!
```

The following example shows the configuration of VMI in aggregate mode using IPv4 and IPv6 as the routing protocols:

```
interface Virtual-Template1
 ip unnumbered vmi1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ip address 2.2.2.1 255.255.255.0
 ipv6 enable
 physical-interface FastEthernet 0/0
!
```

The following example shows the configuration of VMI in aggregate mode using IPv6 as the routing protocol:

```
interface Virtual-Template1
 ipv6 enable
 service-policy output FQ
!
interface vmi1
 ipv6 enable
 physical-interface FastEthernet 0/0
!
```

Examples: Enabling Multicast Support with Bypass or Aggregate Mode

Note The IPv4 address that you configure on the virtual multipoint interface (VMI) is not advertised or used; instead the IPv4 address on the virtual template is used.

Example: Bypass Mode on VMIs for Multicast Traffic

The following example shows how to enable multicast on virtual multipoint interfaces (VMIs). The example includes changing the VMI to bypass mode and enabling Protocol Independent Multicast (PIM) sparse mode on the virtual-template interface:

```
Device# enable
Device# configure terminal
!
Device(config)# interface Virtual-Template1
Device(config-if)# ip address 209.165.200.227 255.255.255.224
Device(config-if)# load-interval 30
Device(config-if)# no keepalive
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# service-policy output FQ
!
!
Device(config)# interface vmi1
Device(config-if)# ip address 10.3.9.1 255.255.255.0
Device(config-if)# load-interval 30
Device(config-if)# physical-interface FastEthernet 0/0
Device(config-if)# mode bypass
!
Device(config)# end
```

Example: EIGRP for IPv4 Using Bypass Mode

The following example shows how to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 using bypass mode. In this example, the IP address of the virtual multipoint interface,VMI1, needs to be defined, but the interface is not routable because the VMI is configured as down/down:

```
hostname host1
!
no aaa new-model
clock timezone EST -5
ip cef
!
no ip domain lookup
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
!
!bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
ip address 209.165.200.225 255.255.255.224
 load-interval 30
!
interface FastEthernet 0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial 1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/2
 no ip address
 no ip mroute-cache
shutdown
 clock rate 2000000
!
interface Serial 1/3
no ip address
 no ip mroute-cache
 shutdown
```

```
 clock rate 2000000
!
interface FastEthernet 2/0
 switchport access vlan 2
 duplex full
speed 100
!
interface FastEthernet 2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet 2/2
 shutdown
!
interface FastEthernet 2/3
 shutdown
!
interface Virtual-Template1
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.225 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
ipv6 enable
!
interface vmi1
ip address 209.165.200.226 255.255.255.224
 load-interval 30
 physical-interface FastEthernet 0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 209.165.200.225 255.255.255.224
 network 209.165.200.226 255.255.255.224
```

Example: EIGRP for IPv6 Using Bypass Mode

The following example shows how to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 using bypass mode:

```
!
ip cef
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
```

```
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
!
archive
 log config
!
!
policy-map FQ
class class-default
 fair-queue
!
!
!
bba-group pppoe VMI1
 virtual-template 1
service profile host1
!
!
interface Loopback1
load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet 0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial 1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/1
 no ip address
 no ip mroute-cache
 shutdown
clock rate 2000000
!
interface Serial 1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet 2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet 2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet 2/2
 shutdown
!
```

```
interface FastEthernet 2/3
 shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 no ip address
 no ip mroute-cache
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface Vlan503
 no ip address
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
no ip address
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet 0/0
 mode bypass
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 no shutdown
 redistribute connected
!
!
!
```

Example: EIGRP with IPv4 and IPv6 Traffic Using Bypass Mode

The following example shows how to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) with IPv4 and IPv6 using bypass mode:

```
!
hostname host1
!
enable
configure terminal
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
```

```
multilink bundle-name authenticated
no virtual-template subinterface
!
archive
 log config
!
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
!
interface Loopback1
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet 0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 pppoe enable group VMI1
!
interface Serial 1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/2
no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet 2/0
 switchport access vlan 2
 duplex full
 speed 100
!
interface FastEthernet 2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet 2/2
 shutdown
!
interface FastEthernet 2/3
 shutdown
!
interface Virtual-Template1
```

```
 ip address 209.165.200.225 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 ip address 209.165.200.226 255.255.255.224
 no ip mroute-cache
 load-interval 30
!
interface Vlan503
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 eigrp 1
!
interface vmi1
 ip address 209.165.200.226 255.255.255.224
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet 0/0
 mode bypass
!
router eigrp 1
 redistribute connected
 network 209.165.200.226 255.255.255.224
 network 209.165.200.227 255.255.255.224
 auto-summary
!
!
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 eigrp router-id 10.9.1.1
 no shutdown
 redistribute connected
!
!
!
end
```

Example: OSPFv3 for Multicast Traffic Using Aggregate Mode

In this example, multicast is configured as a nonbroadcast multiple access (NBMA) network. To configure multicast, the **ip multicast-routing** global configuration command is required. To configure the virtual multipoint interface (VMI) in aggregate mode for multicast, you must configure the VMI with the **ip PIM nbma-mode** command. The following example shows the VMI on an Open Shortest Path First version 3 (OSPFv3) network:

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mcrtr4
!
boot-start-marker
boot-end-marker
```

```
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
!
ip source-route
!
!
ip cef
!
!
ip domain name yourdomain.com
ip multicast-routing
ip multicast cache-headers
no ipv6 cef
subscriber authorization enable
!
subscriber profile chan
 pppoe service manet_radio
!
!
multilink bundle-name authenticated
!username lab privilege 15 secret 5 $1$v1bl$B5KD7o3jVKYqfoKoS0FUJ1
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
bba-group pppoe chan
 virtual-template 1
 service profile chan
!
!
interface Loopback0
 ip address 15.15.15.15 255.255.255.255
 ip broadcast-address 0.0.0.0
!
interface FastEthernet 0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address 1.1.1.2 255.255.255.0
 ip broadcast-address 0.0.0.0
 ip pim sparse-mode
 ip igmp version 3
 duplex auto
 speed auto
!
interface FastEthernet 0/1
 no ip address
 ip broadcast-address 0.0.0.0
 duplex auto
 speed auto
 pppoe enable group chan
!
interface FastEthernet 0/0/0
!
interface FastEthernet 0/0/1
!
interface FastEthernet 0/0/2
!
interface FastEthernet 0/0/3
interface FastEthernet 0/1/0
 no ip address
 ip broadcast-address 0.0.0.0
 duplex auto
 speed auto
!
```

```
interface Virtual-Template1
 ip unnumbered vmi1
 no peer default ip address
 fair-queue
!
interface Vlan1
 ip address 10.15.60.53 255.255.255.0
!
interface vmi1
 ip address 2.2.2.2 255.255.255.0
 ip pim nbma-mode
 ip pim sparse-mode
 ip ospf network point-to-multipoint
 load-interval 30
 physical-interface FastEthernet0/1
!
router ospfv3 1
 log-adjacency-changes
 redistribute connected subnets
 redistribute static
 network 1.1.1.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip pim rp-address 16.16.16.16
ip pim register-source vmi1
!
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 110 permit ip any any
!
!
!
!
control-plane
!
!
!
!
mgcp fax t38 ecm
!
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 inprivilege level 15
 login local
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet ssh
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Example: OSPFv3 for IPv6 Multicast Traffic Using Bypass Mode

```
hostname host1
!
```

```
enable
configure terminal
!
no aaa new-model
clock timezone EST -5
!
!
!
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
subscriber authorization enable
!
subscriber profile host1
 pppoe service manet_radio
!
multilink bundle-name authenticated
no virtual-template subinterface
!
!
archive
 log config
!
policy-map FQ
 class class-default
  fair-queue
!
bba-group pppoe VMI1
 virtual-template 1
 service profile host1
!
interface Loopback1
 no ip address
 load-interval 30
 ipv6 address 2001:0DB1::1/64
 ipv6 enable
!
interface FastEthernet 0/0
 no ip address
 no ip mroute-cache
 load-interval 30
 speed 100
 full-duplex
 ipv6 enable
 pppoe enable group VMI1
!
interface Serial 1/0
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/1
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/2
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface Serial 1/3
 no ip address
 no ip mroute-cache
 shutdown
 clock rate 2000000
!
interface FastEthernet 2/0
 switchport access vlan 2
```

```
 duplex full
 speed 100
!
interface FastEthernet 2/1
 switchport access vlan 503
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet 2/2
 shutdown
!
interface FastEthernet 2/3
shutdown
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
!
ipv6 ospf network point-to-multipoint
ipv6 ospf cost dynamic
 ipv6 ospf 1 area 0
 no keepalive
 service-policy output FQ
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan2
 no ip address
 no ip mroute-cache
load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Vlan503
 load-interval 30
 ipv6 address 2001:0DB8::/32
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface vmi1
 no ip address
 load-interval 30
 ipv6 enable
 physical-interface FastEthernet 0/0
 mode bypass
!
!
no ip http server
no ip http secure-server
!ipv6 router ospf 1
 log-adjacency-changes
 redistribute connected metric-type 1
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Multicast commands	Cisco IOS Multicast Command Reference
Enhanced Interior Gateway Routing Protocol (EIGRP) configuration tasks and commands	*IP Routing: EIGRP Configuration Guide* Cisco IOS IP Routing: EIGRP Command Reference
Open Shortest Path First (OSPF) configuration tasks and commands	*IP Routing: OSPF Configuration Guide* Cisco IOS IP Routing: OSPF Command Reference
IPv6 configuration tasks and commands	*IPv6 Configuration Library* Cisco IOS IPv6 Command Reference

Technical Assistance

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

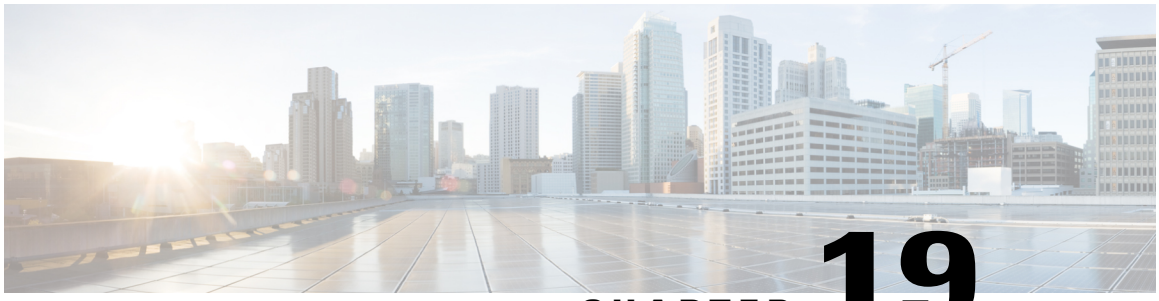
Feature Information for Multicast for Virtual Multipoint Interfaces

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

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

Table 14: Feature Information for Multicast for Virtual Multipoint Interfaces

Feature Name	Releases	Feature Information
Multicast for Virtual Multipoint Interfaces	15.1(3)T	The Multicast for Virtual Multipoint Interfaces feature enables multicast support for RFC 5578-compliant Radio-Aware Routing. No new or modified commands were introduced with this feature.



CHAPTER 19

OSPFv3 Dynamic Interface Cost Support

The Open Shortest Path First version 3 (OSPFv3) Dynamic Interface Cost Support feature provides enhancements to the OSPFv3 cost metric in Mobile Ad Hoc Network (MANET) environments. This feature enables the route cost to a neighbor to be dynamically updated based on metrics reported by the radio,allows the best route to be chosen within a given set of radio links, and reduces the effect of frequent routing changes.

Finding Feature Information

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

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

Information About OSPFv3 Dynamic Interface Cost Support

Link-Quality Metrics Reporting for OSPFv3

The quality of a radio link has a direct impact on the throughput that can be achieved by device-to-device traffic. The PPP over Ethernet (PPPoE) provides a process by which a device can request, or a radio can report, link-quality metric information. With the Cisco Open Shortest Path First version 3 (OSPFv3) implementation, the route cost to a neighbor is dynamically updated based on metrics reported by the radio, thus allowing the best route to be chosen within a given set of radio links and reducing the effect of frequent routing changes.

The routing protocols receive raw radio-link data and compute a composite quality metric for each link In computing these metrics, you should consider these factors:

- Maximum data rate—the theoretical maximum data rate of the radio link, in scaled bits per second
- Current data rate—the current data rate achieved on the link, in scaled bits per second
- Resources—a percentage (0 to 100) that can represent the remaining amount of a resource (such as battery power)
- Latency—the transmission delay packets encounter, in milliseconds
- Relative link quality—a numeric value (0 to 100) representing relative quality, with 100 being the highest quality

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100 percent and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPF cost.

You can weight metrics during the configuration process to emphasize or deemphasize particular characteristics. For example, if throughput is a particular concern, you can weight the *throughput* metric so that it is factored more heavily into the composite route cost. Similarly, a metric of no concern can be omitted from the composite calculation.

Because cost components can change rapidly, you might need to dampen the number of changes to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

Link metrics can change rapidly, often by very small degrees, which can result in a flood of meaningless routing updates. In a worst-case scenario, the network could churn almost continuously as it struggles to react to minor variations in link quality. To alleviate this concern, Cisco provides a tunable dampening mechanism that allows you to configure threshold values. Any metric change that falls below the threshold is ignored. The quality of a connection to a neighbor varies, based on various characteristics of the interface when OSPFv3 is used as the routing protocol. The routing protocol receives dynamic raw radio-link characteristics and computes a composite metric that is used to reduce the effect of frequent routing changes.

By using the tunable hysteresis mechanism, you can adjust the threshold to the routing changes that occur when the device receives a signal that a new peer has been discovered or that an existing peer is unreachable. The tunable metric is weighted and is adjusted dynamically to account for these characteristics:

- Current and maximum bandwidth
- Latency
- Resources
- Relative link quality (RLQ)

You can deconfigure individual weights, and you can clear all weights so that the cost returns to the default value for the interface type. Based on the routing changes that occur, you can determine the cost by applying these metrics. For more information about the **ipv6 ospf cost** command, see the *Cisco IOS IPv6 Command Reference*.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Open Shortest Path First (OSPF) commands	Cisco IOS IP Routing: OSPF Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference

Technical Assistance

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

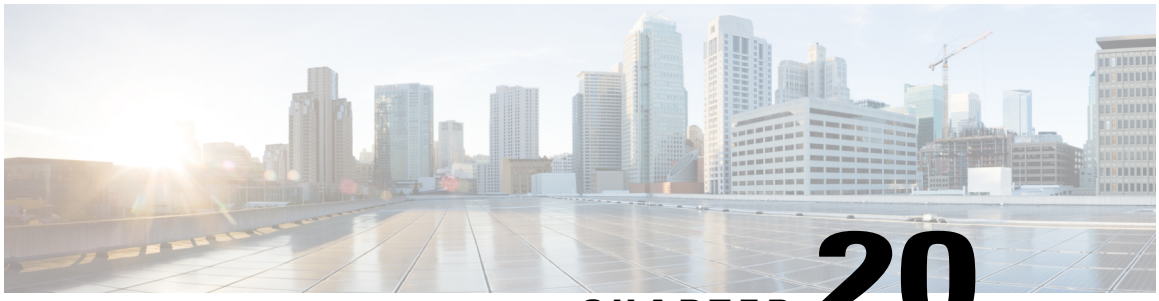
Feature Information for OSPFv3 Dynamic Interface Cost Support

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

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

Table 15: Feature Information for OSPFv3 Dynamic Interface Cost Support

Feature Name	Releases	Feature Information
OSPFv3 Dynamic Interface Cost Support	12.4(15)XF 12.4(15)T 15.0(1)M	OSPFv3 Dynamic Interface Cost Support provides enhancements to the Open Shortest Path First version 3 (OSPFv3) cost metric for supporting Mobile Ad Hoc Networks (MANETs). The following commands were introduced or modified: **debug ipv6 ospf l2api**, **ipv6 ospf cost**, **test ospfv3 interface**.



CHAPTER 20

VMI QoS

The VMI QoS feature supports full modular quality of service (QoS) CLI (MQC) configurations on virtual multipoint interfaces. QoS configurations include remarking, shaping, and policing.

The VMI provides services that map outgoing packets to the appropriate PPP over Ethernet (PPPoE) sessions based on the next-hop forwarding address for that packet.

Finding Feature Information

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

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

Restrictions for VMI QoS

You can apply the quality of service (QoS) policy to only one outgoing interface that the PPP over Ethernet (PPPoE) session is traversing.

Information About VMI QoS

VMI QoS

Virtual multipoint interfaces (VMIs) support full modular quality of service (QoS) CLI (MQC) configurations, which includes remarking, shaping, and policing. For details, see the *QoS Modular QoS Command-Line Interface Configuration Guide* publication that is part of the *Quality of Service Solutions Configuration Guide Library*.

Configuration Examples for VMI QoS

Examples: QoS Configuration for VMI

The following example shows a configuration for quality of service (QoS) features:

```
class-map match-any chat
 match dscp af11
class-map match-any voice
 match dscp ef
class-map match-any af23
 match dscp af23
class-map match-any af31
 match dscp af31
class-map match-any af33
 match dscp af33
class-map match-any af42
 match dscp af42
policy-map multiple_sessions
 class chat
 bandwidth 50
 class voice
 bandwidth 100
 class af23
 bandwidth 150
 class af31
 bandwidth 200
 class af33
 bandwidth 250
 class af42
 bandwidth 300
 interface virtual-template 1
service-policy output multiple_sessions
```

The following example shows a configuration for shaping:

```
class-map match-any chat
match dscp af11
class-map match-any voice
match dscp ef
policy-map shape_child
class chat
bandwidth 200
class voice
priority 100
policy-map shape_parent
class class-default
shape average 400000
service-policy shape_child
```

The following example shows a configuration for assigning a policy to a virtual multipoint interface (VMI):

```
interface vmi1
service-policy output shape_parent
```

The following example shows a configuration for policing actions:

```
class-map match-any af12
match dscp af12
class-map match-any af41
match dscp af41
policy-map police
class af12
police 1000000 conform-action set-dscp-transmit af31 exceed-action set-dscp-transmit af23
violate-action set-dscp-transmit af23
class af41
police 1000000 conform-action transmit exceed-action drop violate-action drop
```

The following example shows a configuration for assigning a policy to a virtual template interface:

```
interface virtual-template 1
service-policy output police
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Quality of service (QoS) commands	Cisco IOS Quality of Service Solutions Command Reference
Modular QoS CLI (MQC) configuration	*QoS Modular QoS Command-Line Interface Configuration Guide* (part of the *Quality of Service Solutions Configuration Guide Library*)

Technical Assistance

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

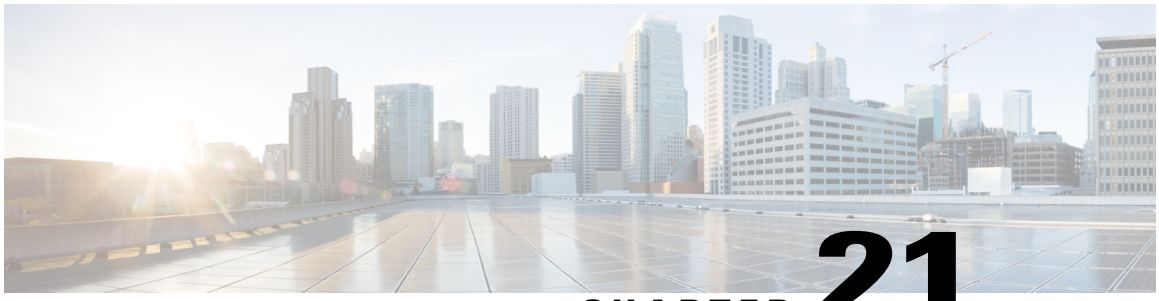
Feature Information for VMI QoS

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

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

Table 16: Feature Information for VMI QoS

Feature Name	Releases	Feature Information
VMI QoS	15..2(1)T	The virtual multipoint interface (VMI) supports full modular quality of service (QoS) CLI (MQC) configurations, which includes remarking, shaping, and policing. No commands were introduced or modified.



CHAPTER 21

Multi-VRF for NEMO

Multi-VRF NEMO feature enables user privacy and supports overlapping IP addresses on a network mobility (NEMO) mobile router so that the devices or subnets connected to the NEMO mobile router seamlessly access multiple enterprise virtual routing and forwarding instances (VRFs), or multiple separate services across an access point name (APN).

Finding Feature Information

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

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

Information About Multi-VRF NEMO

Dynamic Mobile Network Routing

Dynamic Mobile Network Routing (DMNR) is a network-based, mobile technology that provides dynamic routing, and support for mobile or stationary enterprise routers in primary wireless access or automatic wireless

backup configurations. DMNR enables integration between wireless and wireline enterprise services that is, third generation (3G)Wireless WAN, by making use of the Mobile IPv4 network mobility (NEMO) protocol.

The mobile router is used with DMNR service for providing backup communications over Code Division Multiple Access (CDMA) or Evolution-Data Optimized (EVDO) Access and mobile private networks between an enterprise branch office and a data center connected to a IP MPLS/VPN network.

Multi-VRF NEMO feature enables privacy and supports overlapping IP addresses on a network mobility (NEMO) mobile router so that the devices or subnets connected to the NEMO mobile router seamlessly access multiple enterprise virtual routing and forwarding instances (VRFs), or multiple separate services across an access point name (APN).

Per-VRF Tunnel Template Support

Tunnel template support is available in this feature. A separate tunnel template is configured on a mobile router (MR) for each virtual routing and forwarding (VRF) instance, and the same tunnel template is applied on the tunnel created specifically for each VRF instance. The template is configured before the network mobility (NEMO) call is created.

How to Configure Multi-VRF NEMO

Defining VRF Instances

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv4**
5. **address-family ipv4**
6. **exit**
7. Repeat the steps 3 through 6 to define another VRF instance. You can repeat these steps as many times as the required number of VRF instances.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device (config)# vrf definition red1`	Enters IP VRF configuration mode for defining a VRF routing table instance.
Step 4	**address-family ipv4** **Example:** `Device (config-vrf)# address-family ipv4`	Enters VRF address-family configuration mode to configure a routing session using standard IPv4 address prefixes.
Step 5	**address-family ipv4** **Example:** `Device (config-vrf-af)# exit-address-family`	Exits VRF address-family configuration mode and enters IP VRF configuration mode.
Step 6	**exit** **Example:** `Device (config-vrf)# exit`	Exits IP VRF configuration mode and enters global configuration mode.
Step 7	Repeat the steps 3 through 6 to define another VRF instance. You can repeat these steps as many times as the required number of VRF instances.	—

Configuring Multi-VRF for NEMO

Before You Begin

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile router**
4. **address** *address mask*
5. **address** *address mask*
6. **home-agent** *ip-address* [**priority** *level*]
7. **mobile-network** *interface interface-number*
8. **mobile-network** *interface interface-number*
9. **vrf-routing** *vrf-name*
10. **vrf-routing** *vrf-name*
11. **template tunnel** *interface-number* [**vrf** *vrf-name*]
12. **template tunnel** *interface-number* [**vrf** *vrf-name*]
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 3	**ip mobile router** **Example:** `Device> ip mobile router`	Enables the mobile router and enters mobile router configuration mode.
Step 4	**address** *address mask* **Example:** `Device (mobile-router)# ip mobile router`	Enables the mobile router and enters mobile router configuration mode.

	Command or Action	Purpose
Step 5	**address** *address mask* **Example:** `Device (mobile-router)# address 10.2.2.2 255.255.255.255`	Sets an IP address for the tunnel source interface.
Step 6	**home-agent** *ip-address* [**priority** *level*] **Example:** `Device (mobile-router)# home-agent 10.1.1.1`	Specifies the home agent that the mobile router uses during registration.
Step 7	**mobile-network** *interface interface-number* **Example:** `Device (mobile-router)# mobile-network Ethernet 0/3`	Specifies the mobile router interface that is connected to the dynamic mobile network.
Step 8	**mobile-network** *interface interface-number* **Example:** `Device (mobile-router)# mobile-network Ethernet 1/1`	Specifies the mobile router interface that is connected to the dynamic mobile network.
Step 9	**vrf-routing** *vrf-name* **Example:** `Device (mobile-router)# vrf-routing red1`	Enables the mobile router carry the network prefixes belonging to a VRF in the registration request message.
Step 10	**vrf-routing** *vrf-name* **Example:** `Device (mobile-router)# vrf-routing blue1`	Enables the mobile router carry the network prefixes belonging to a VRF in the registration request message.
Step 11	**template tunnel** *interface-number* [**vrf** *vrf-name*] **Example:** `Device (mobile-router)# template tunnel 200 vrf red1`	Applies a tunnel template to tunnels brought up in a specific VRF or global VRF at the mobile router.
Step 12	**template tunnel** *interface-number* [**vrf** *vrf-name*] **Example:** `Device (mobile-router)# template tunnel 200 vrf blue1`	Applies a tunnel template to tunnels brought up in a specific VRF or global VRF at the mobile router.
Step 13	**end** **Example:** `Device (mobile-router)# end`	Exits the mobile router configuration and returns to privileged EXEC mode.

Configuration Examples for Multi-VRF for NEMO

Example: Defining VRF Instances

```
Device> enable
Device# configure terminal
Device(config)# vrf definition red1
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# vrf definition red1
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# end
```

Example: Configuring Multi-VRF for NEMO

```
Device> enable
Device# configure terminal
Device(config)# ip mobile router
Device(mobile-router)# ip mobile router
Device(mobile-router)# home-agent 10.1.1.1
Device(mobile-router)# mobile-network Ethernet 0/3
Device(mobile-router)# mobile-network Ethernet 1/1
Device(mobile-router)# vrf-routing red1
Device(mobile-router)# vrf-routing blue1
Device(mobile-router)# template tunnel 200 vrf red1
Device(mobile-router)# template tunnel 200 vrf blue1
Device(mobile-router)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IP Mobility commands	Cisco IOS IP Mobility Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Multi-VRF for NEMO

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

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

Table 17: Feature Information for Multi-VRF for NEMO

Feature Name	Releases	Feature Information
Multi-VRF for NEMO	15.4(3)T	The Multi-VRF NEMO feature enables privacy and supports overlapping IP addresses on a network mobility (NEMO) mobile router so that the devices or subnets connected to the NEMO mobile router seamlessly access multiple enterprise virtual routing and forwarding instances (VRF)s, or multiple separate services across an access point name (APN). The following commands were introduced or modified: **template tunnel**, **vrf-routing**, **test ospfv3 interface**.

INDEX

I

R