

Cisco Mobile IP



Executive Summary

Two of the world's most powerful technology trends, the Internet and mobile communications, are redefining how and when people access information. With the majority of information and new services being deployed over IP, the use of devices such as cellular phones, Personal Digital Assistants (PDAs) and laptops for accessing data networks is pushing the need for "always on" IP connectivity. Clearly, these connections are valuable. The evolution of mobile computing points to a coming together of the best of desktop computing and cellular communications—the predictability and "always connected" experience of the desktop combined with the ease of use and mobility of the cell phone.

The number of wireless devices for voice or data is projected to surpass the number of fixed devices. Mobile data communication will likely emerge as the technology supporting most communication including voice and video. Mobile data communication will be pervasive in cellular systems such as 3G, and in wireless LAN such as 802.11, and will extend into satellite communication. Though mobility may be enabled by link-layer technologies, data crossing networks or different link layers is still a problem. The solution to this problem is a standards-based protocol: Mobile IP.

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

Cisco IOS[®] Software and its support for Mobile IP provide the technology that enables an IP node's ability to retain the same IP address and maintain existing communications while traveling from one network to another.

Mobile IP eliminates a stop-and-start approach to IP connectivity that is required with network location changes, thus enabling users to maintain the same IP address regardless of their point of attachment to the network. This document provides an introduction to Mobile IP.

Mobile IP Overview

In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to a fixed address on an envelope. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network.

However, problems occur when a device roams away from its home network and is no longer reachable using normal IP routing. This causes the active sessions of the device to be terminated. Mobile IP enables users to keep the same IP address while traveling to a different network (which may even be operated by a different wireless operator), thus ensuring that a roaming individual can continue communication without sessions or connections being dropped.

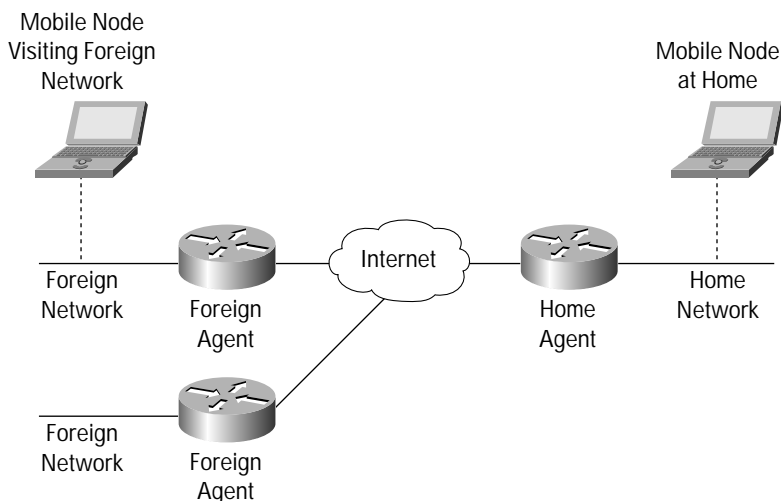
Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of wireless and wireline networks while maintaining connections and ongoing applications. Remote login, remote printing, and file transfers are examples of applications where it is undesirable to interrupt communications while an individual roams across network boundaries. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses can compromise the network services.

Components of a Mobile IP Network

Mobile IP has the following three components (Figure 1):

- Mobile node
- Home agent
- Foreign agent

Figure 1 Mobile IP Components and Relationships



The Mobile Node is a device such as a cell phone, PDA, or laptop whose software enables network roaming capabilities.

The Home Agent is a router on the home network serving as the anchor point for communication with the Mobile Node; it tunnels packets from a device on the Internet, called a Correspondent Node, to the roaming Mobile Node. (A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network.)

The Foreign Agent is a router that can function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

The care-of address is the termination point of the tunnel toward the Mobile Node when it is on a foreign network. The Home Agent maintains an association between the home IP address of the Mobile Node and its care-of address, which is the current location of the Mobile Node on the foreign or visited network.



How Mobile IP Works

The Mobile IP process has three main phases, which are discussed in the following sections.

- Agent Discovery—A Mobile Node discovers its Foreign and Home Agents during agent discovery.
- Registration—The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.
- Tunneling—A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

Agent Discovery

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

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

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

- Care-of address acquired from a Foreign Agent
- Collocated care-of address

A Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node. A Mobile Node that acquires this type of care-of address can share the address with other Mobile Nodes. A collocated care-of address is an IP address temporarily assigned to the interface of the Mobile Node 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.

When the Mobile Node hears a Foreign Agent advertisement and detects that it has moved outside of its home network, it begins registration.

Registration

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

The Mobile Node uses this information along with the information that it learns from the Foreign Agent advertisements to form a Mobile IP registration request. It adds the registration request to its pending list and sends the registration request to its Home Agent either through the Foreign Agent or directly if it is using a collocated care-of address and is not required to register through the Foreign Agent. If the registration request is sent through the Foreign Agent, the Foreign Agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported. If the registration request is valid, the Foreign Agent adds the visiting Mobile Node to its pending list before relaying the request to the Home Agent. If the registration request is not valid, the Foreign Agent sends a registration reply with appropriate error code to the Mobile Node.

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

The Home Agent then sends a registration reply to the Mobile Node through the Foreign Agent (if the registration request was received via the Foreign Agent) or directly to the Mobile Node. If the registration request is not valid, the Home Agent rejects the request by sending a registration reply with an appropriate error code.

The Foreign Agent checks the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the Foreign Agent adds the Mobile Node to its visitor list, establishes a tunnel to the Home Agent if reverse tunnel is enabled, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the Mobile Node.

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

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

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

Tunneling

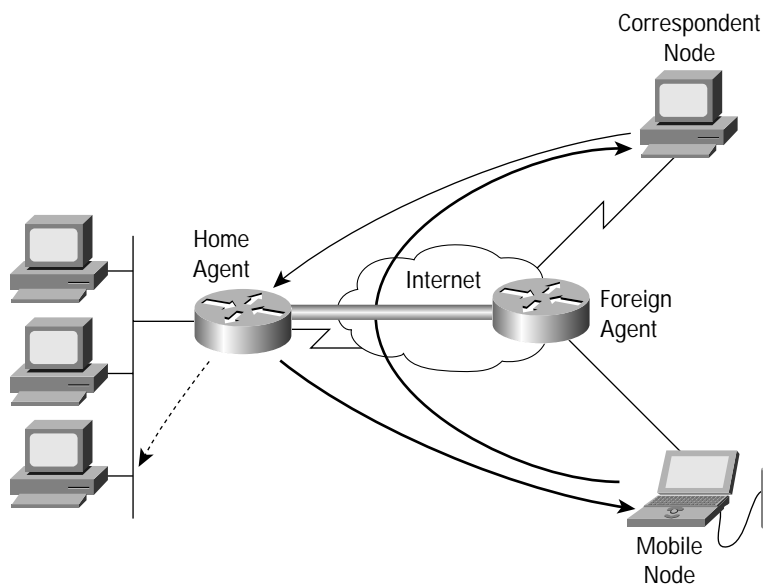
The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes.

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



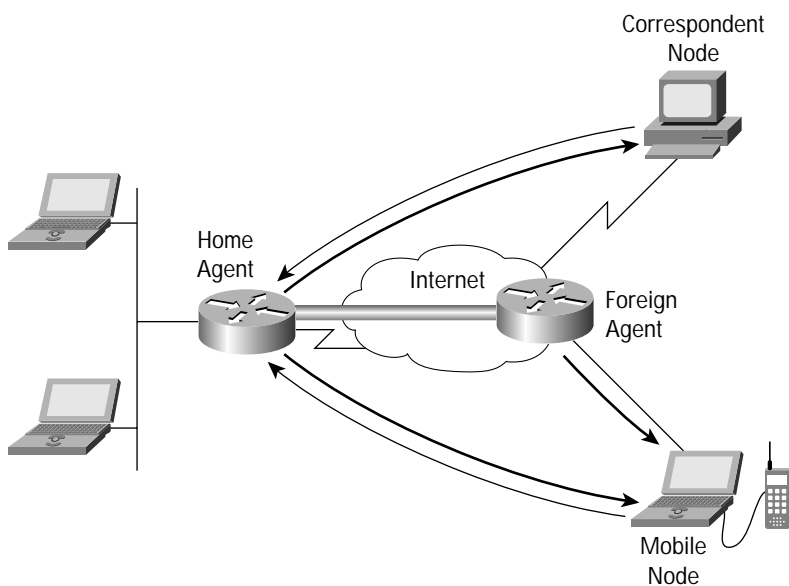
Typically, the Mobile Node sends packets to the Foreign Agent, which routes them to their final destination, the Correspondent Node (Figure 2).

Figure 2 Packet Forwarding



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

Figure 3 Reverse Tunnel



Security

Mobile IP uses a strong authentication scheme for security purposes. All registration messages between a Mobile Node and Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE).

The integrity of the registration messages is protected by preshared 128-bit key between a Mobile Node and Home Agent. The keyed message digest algorithm 5 (MD5) in “prefix+suffix” mode is used to compute the authenticator value in the appended MHAE, which is mandatory. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a Mobile Node and Foreign Agent and between a Foreign Agent and Home Agent, respectively.

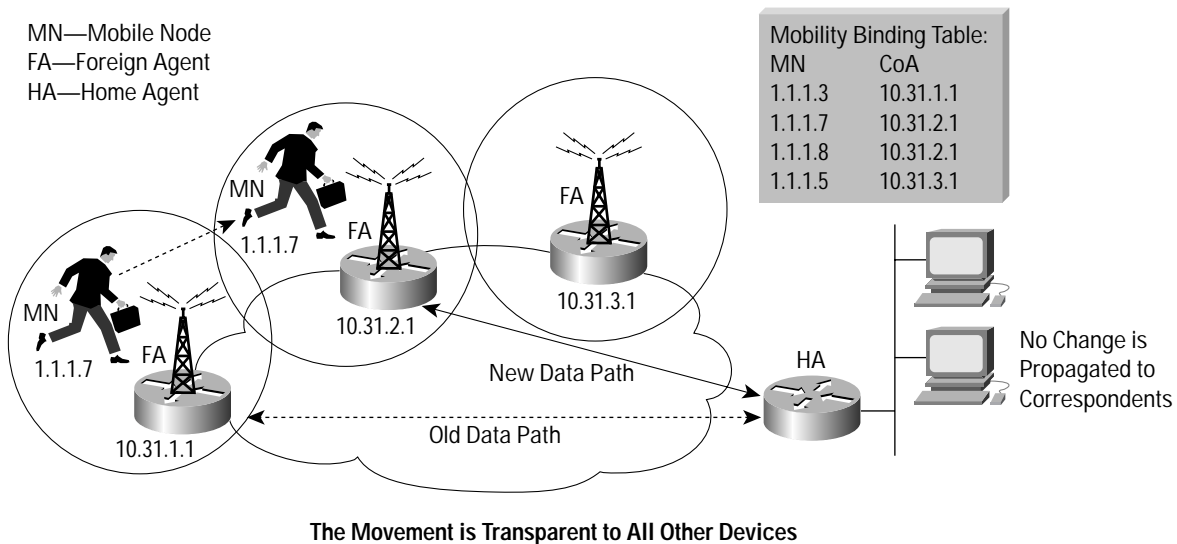
Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The Home Agent returns its time stamp to synchronize the Mobile Node for registration.

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.

Solution to Network Mobility

Network mobility is enabled by Mobile IP, which provides a scalable, transparent, and secure solution. It is scalable because only the participating components need to be Mobile IP aware—the Mobile Node and the endpoints of the tunnel. No other routers in the network or any hosts with which the Mobile Node is communicating need to be changed or even aware of the movement of the Mobile Node. It is transparent to any applications while providing mobility. Also, the network layer provides link-layer independence, interlink layer roaming, and link-layer transparency. Finally, it is secure because the set up of packet redirection is authenticated.

Figure 4 Roaming with Mobile IP





Because a mobile user is able to maintain the same IP address even while roaming across networks, a live IP connection can be maintained without having to stop and restart as it would with a mechanism such as Dynamic Host Configuration Protocol (DHCP). This is the real power of Mobile IP: it offers the potential to leverage Mobile IP with applications such as voice over IP (VoIP) and streaming media (video) to IP devices while a user is enroute or changes location.

Applications:

- Enables seamless movement while “always on” in a corporate campus environment between floors and buildings using technologies such as 802.11 or across multiple service provider networks and hot spots, for example, spanning technologies such as CDMA and 802.11.
- Enables applications such as Telematics—Convergence of wireless communications and IT for in-vehicle communication that makes a moving vehicle a part of a network thereby allowing different applications to run seamlessly across different types of wireless technologies and different characteristics of the links. Enables always-on connectivity for users traveling in railroads, cruise liners, planes, and so on. Also very useful for sharing control and routing information in these environments.
- Enables mission-critical applications for public safety agencies such as ambulances, the Coast Guard, police, and so on to stay connected to the network while on the move. EMS vehicles already have numerous IP devices, so a mobile router can provide transparent communications between EMS vehicles and hospitals.

Related Documents

Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Software Release 12.2

Cisco IOS IP Configuration Guide, Software Release 12.2

For More Information

Additional information about Cisco IOS Mobile IP technology is available at http://www.cisco.com/go/mobile_ip/ or by contacting your local Cisco representative.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0108R) LW2755 10/01

Printed in the USA