Introduction to Mobile IP

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

This section provides an overview of the Mobile IP technology.

Mobile IP Overview

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

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

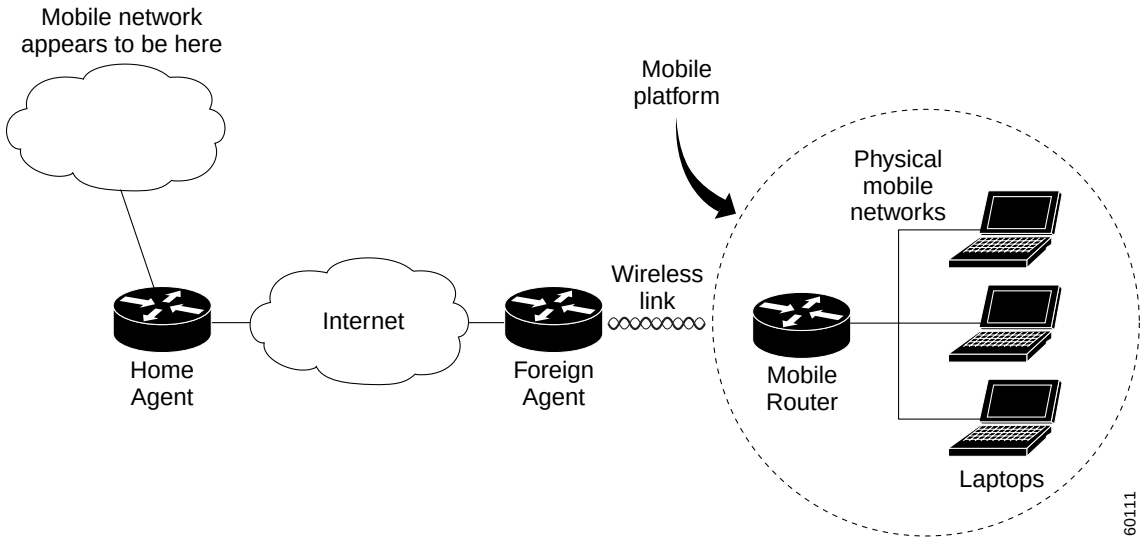
This results in the active sessions of the device being terminated. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication without sessions or connections being dropped.

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

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

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

Figure 3-1 Cisco Mobile Network Components and Relationships



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

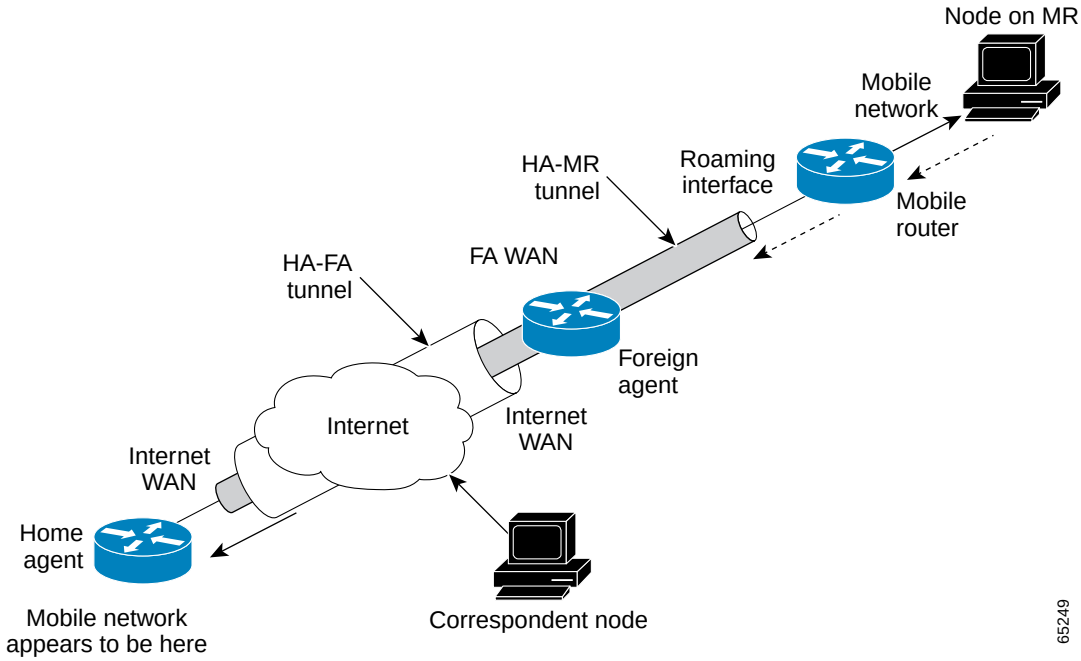
These devices can be mobile nodes without Mobile IP client software. The mobile access router eliminates the need for a Mobile IP client. The mobile access router “hides” the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

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

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

Mobile IP components are shown in Figure 3-2.

Figure 3-2 Mobile IP Components and Relationships



Mobile IP Process

The Mobile IP process has three main phases.

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

Agent Discovery

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

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

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

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

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

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

Registration

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

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

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

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

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

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

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

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

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

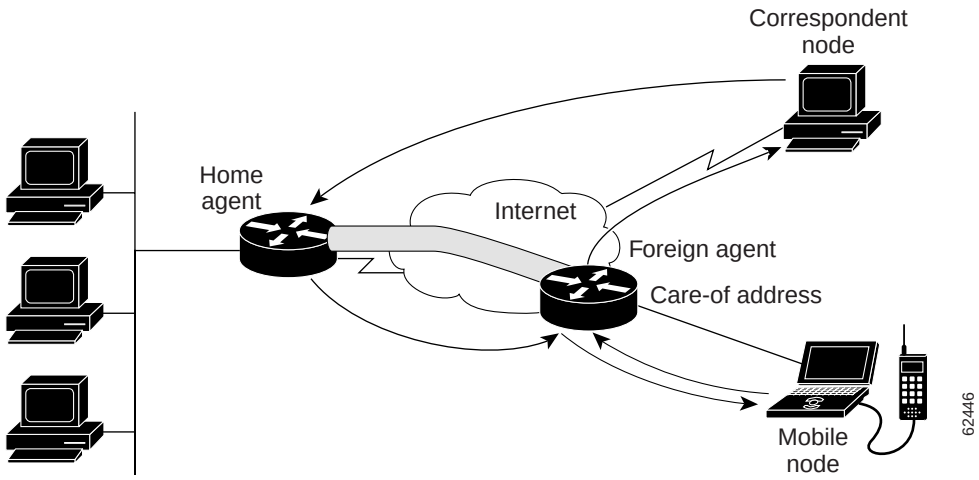
Tunneling

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

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

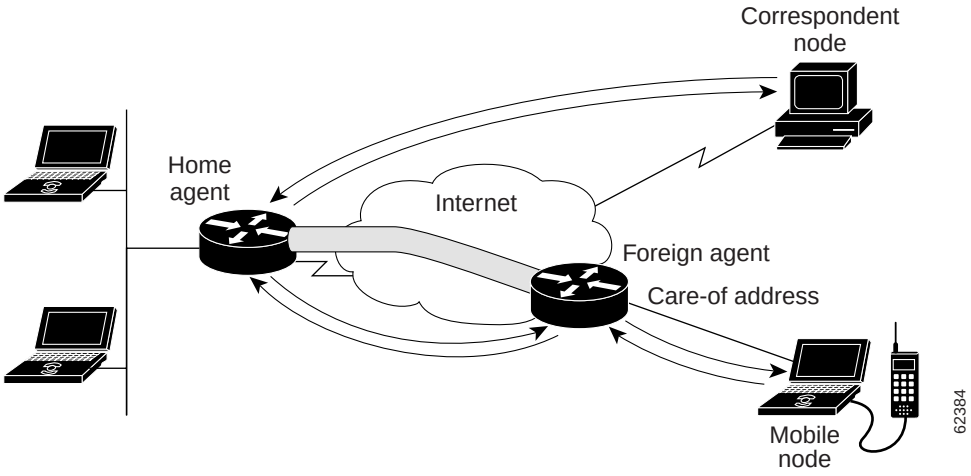
Typically, the mobile node sends packets to the foreign agent, which routes them to their final destination, the Correspondent Node, as shown in Figure 3-3.

Figure 3-3 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. See Figure 3-4.

Figure 3-4 Reverse Tunnel



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

Mobile IP or DHCP

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

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

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