



Configuring Proxy Mobile IP

This chapter describes how to configure your access point's proxy Mobile IP feature. This chapter contains these sections:

- [Understanding Proxy Mobile IP, page 15-2](#)
- [Configuring Proxy Mobile IP, page 15-6](#)

Understanding Proxy Mobile IP

These sections explain how access points conduct proxy Mobile IP:

- [Overview, page 15-2](#)
- [Components of a Proxy Mobile IP Network, page 15-2](#)
- [How Proxy Mobile IP Works, page 15-3](#)
- [Proxy Mobile IP Security, page 15-6](#)

Overview

The access point's proxy Mobile IP feature works in conjunction with the Mobile IP feature in IOS. When you enable proxy Mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks. The visiting client devices do not need special software; the access point provides proxy Mobile IP services on their behalf. Any wireless client can participate.

Mobile IP provides users the freedom to roam beyond their home subnets while maintaining their home IP addresses. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam. For example, a client device with an IP address of 192.95.5.2 could associate to an access point on a network whose IP addresses are in the 209.165.200.x range. The guest client device keeps its 192.95.5.2 IP address, and the access point forwards its packets through a Mobile IP enabled router across the Internet to a router on the client's home network.

Access points with proxy Mobile IP enabled attempt to provide proxy service for any client device that associates and does not perform the following:

- Does not issue a DHCP request to get a new IP address.
- Does not support a Mobile IP stack. If a device supports a Mobile IP stack, the access point assumes that the device will perform its own Mobile IP functions.

You enable proxy Mobile IP for specific SSIDs on the access point, providing support only for clients that use those SSIDs. Proxy Mobile IP does not support VLANs. You can pause proxy Mobile IP support without losing your proxy Mobile IP configuration.

Proxy Mobile IP is disabled by default.

**Note**

Guest client devices do not receive broadcast and multicast packets.

Components of a Proxy Mobile IP Network

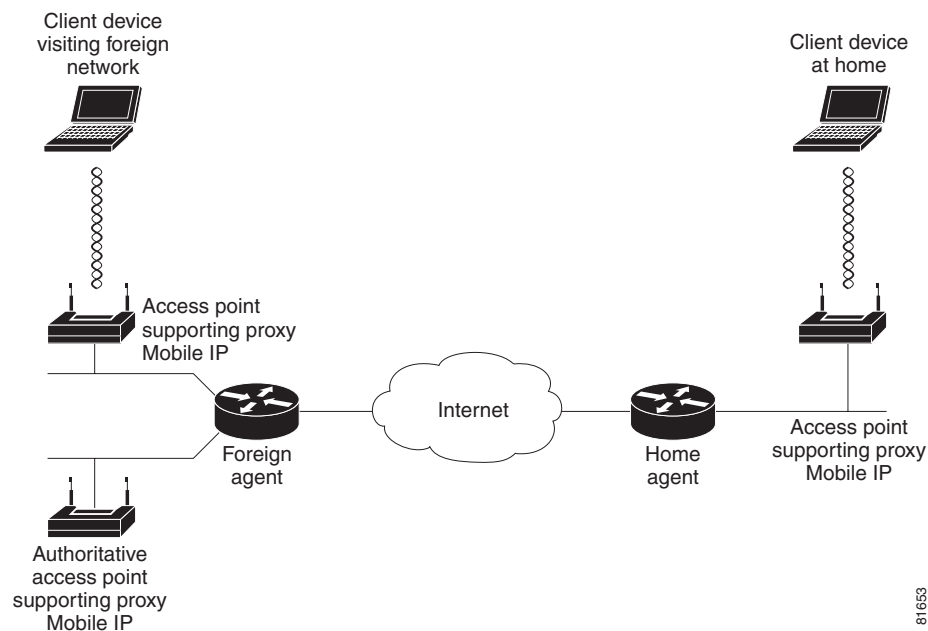
Five devices participate in proxy Mobile IP:

- A visiting client device. The visiting client device is any device such as a personal digital assistant or a laptop that can associate to a wireless access point. It does not need any special proxy Mobile IP software.
- An access point with proxy Mobile IP enabled. The access point proxies on behalf of the visiting client device, performing all Mobile IP services for the device.

- An authoritative access point on your network supporting proxy Mobile IP. The authoritative access point uses a subnet map to keep track of the home agent information for all visiting client devices.
- A home agent. The home agent is a router on the visiting client's home network that serves as the anchor point for communication with the access point and the visiting client. The home agent tunnels packets from a correspondent node on the Internet to the visiting client device.
- A foreign agent. The foreign agent is a router on your network that serves as the point of attachment for the visiting client device when it is on your network, delivering packets from the home agent to the visiting client.

Figure 15-1 shows the five participating devices.

Figure 15-1 Participating Devices in Proxy Mobile IP



How Proxy Mobile IP Works

The proxy Mobile IP process has four main phases. These sections describe each phase:

- [Agent Discovery, page 15-3](#)
- [Subnet Map Exchange, page 15-4](#)
- [Registration, page 15-5](#)
- [Tunneling, page 15-5](#)

Agent Discovery

During the agent discovery phase, the home agent and the foreign agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The access point listens to these advertisements.

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 client devices. Rather than waiting for agent advertisements, an access point can send out an agent solicitation. This solicitation forces any agents on the network to immediately send an agent advertisement.

When an access point determines that a client device is connected to a foreign network, it acquires a care-of address for the visiting client. The care-of address is an IP address of a foreign agent that has an interface on the network being visited by a client device. An access point can share this address among many visiting client devices.

When the visiting client associates to an access point, the access point compares the client's IP address with that of its own IP network information and detects that the client is a visitor from another network. The access point then begins the registration. However, before the access point can begin the registration process on behalf of the visiting client, it needs to know the home agent IP address of the visiting client. It gets the home agent's IP address by looking it up on a subnet map table.

Subnet Map Exchange

Each access point with proxy Mobile IP enabled maintains a subnet map table. The subnet map table consists of a list of home agent IP addresses and their subnet masks. [Table 15-1](#) is an example of a subnet map table.

Table 15-1 Example of a Subnet Map Table

Home Agent	Subnet Mask
10.10.10.1	255.255.255.0
10.10.4.2	255.255.255.0
10.3.4.4	255.255.255.248
10.12.1.1	255.255.0.0

Access points use the subnet map table to determine the IP address of the visiting client's home agent. When an access point boots up or when proxy Mobile IP is first enabled on an access point, it obtains its own home agent information using the agent discovery mechanism. It sends this information to another access point called an authoritative access point (AAP). The AAP is an access point that is responsible for keeping the latest subnet map table.

When the AAP receives the new information, it replies to the access point with a copy of the latest subnet map table. The new access point now has the latest subnet map table locally and it is ready to perform proxy Mobile IP for visiting clients. Having the subnet map table locally helps the access point do a quick lookup for the home agent information. Meanwhile, the AAP adds the new access point to its list of access points and the home agent information to its subnet map table. The AAP then updates all the other access points with this additional piece of information.

You can designate up to three AAPs on your wireless LAN. If an access point fails to reach the first AAP, it tries the next configured AAP. The AAPs compare their subnet map tables periodically to make sure they have the same subnet map table. If the AAP detects that there are no more access points for a particular home agent, it sends a deregistration packet on behalf of the broadcast address of the home agent subnet to see if the home agent is still active. If the home agent responds, the AAP keeps the home agent entry in the subnet map table even though there are no access points in the home agent's subnet. This process supports client devices that have already roamed to foreign networks. If the home agent does not respond, the AAP deletes the home agent entry from the subnet map table.

When a client device associates to an access point and the access point determines that the client is visiting from another network, the access point performs a longest-match lookup on its subnet map table and obtains the home agent address for the visiting client. When the access point has the home agent address, it can proceed to the registration step.

Registration

The access point is configured with the mobility security association (which includes the shared key) of all potential visiting clients with their corresponding home agents. You can enter the mobility security association information locally on the access point or on a RADIUS server on your network, and access points with proxy Mobile IP enabled can access it there.

The access point uses the security association information, the visiting client's IP address, and the information that it learns from the foreign agent advertisements to form a Mobile IP registration request on behalf of the visiting client. It sends the registration request to the visiting client's home agent 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 and that the requested tunnel encapsulation is available. If the registration request is valid, the foreign agent relays the request to the home agent.

The home agent checks the validity of the registration request, which includes authentication of the visiting client. If the registration request is valid, the home agent creates a mobility binding (an association of the visiting client 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 visiting client through the foreign agent (because the registration request was received through the foreign agent). 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 visiting client 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 visiting client.

Finally, the access point checks the validity of the registration reply. If the registration reply specifies that the registration is accepted, the access point is able to confirm that the mobility agents are aware of the visiting client's roaming. Subsequently, the access point intercepts all packets from the visiting client and sends them to the foreign agent.

The access point re-registers on behalf of the visiting client before its registration lifetime expires. The home agent and foreign agent update their mobility binding and visitor entry, respectively, during re-registration.

A successful Mobile IP registration by the access point on behalf of the visiting client sets up the routing mechanism for transporting packets to and from the visiting client as it roams.

Tunneling

The visiting client sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the visiting client is roaming on foreign networks, its movements are transparent to correspondent nodes (other devices with which the visiting client communicates).

Data packets addressed to the visiting client are routed to its home network, where the home agent intercepts and tunnels them to the care-of address toward the visiting client. 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 tunnel mode that the access point supports is IP Encapsulation within IP Encapsulation.

Typically, the visiting client sends packets as it normally would. The access point intercepts these packets and sends them to the foreign agent, which routes them to their final destination, the correspondent node.

Proxy Mobile IP Security

Mobile IP uses a strong authentication scheme to protect communications to and from visiting clients. All registration messages between a visiting client and the home agent must contain the Mobile-Home Authentication Extension (MHAE). Proxy Mobile IP also implements this requirement in the registration messages sent by the access point on behalf of the visiting clients to the home agent.

The integrity of the registration messages is protected by a shared 128-bit key between the access point (on behalf of the visiting client) and the home agent. You can enter the shared key on the access point or on a RADIUS server.

The keyed message digest algorithm 5 (MD5) in prefix+suffix mode is used to compute the authenticator value in the appended MHAE. Mobile IP and proxy Mobile IP also support 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 the Foreign-Home Authentication Extension are appended to protect message exchanges between a visiting client 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 visiting client for registration. In proxy Mobile IP, the visiting clients are not synchronized to their home agents because the access point intercepts all home agent messages.

Configuring Proxy Mobile IP

These sections describe how to configure proxy Mobile IP:

- [Configuration Guidelines, page 15-6](#)
- [Configuring Proxy Mobile IP on Your Wired LAN, page 15-7](#)
- [Configuring Proxy Mobile IP on Your Access Point, page 15-7](#)

Configuration Guidelines

Before configuring proxy Mobile IP, you should consider these guidelines:

- You can enable proxy Mobile IP only on root access points (units connected to the wired LAN). You cannot enable proxy Mobile IP on repeater access points.
- Access points participating in proxy Mobile IP should be configured with gateway addresses. You can configure the gateways manually, or the access points can receive gateways through DHCP.
- The foreign and home agents must reside on the network gateways where you want to support proxy Mobile IP.
- If your authoritative access points receive their IP addresses through DHCP, use the access point host names to specify the AAPs in the proxy Mobile IP configuration.
- Proxy Mobile IP does not support broadcast and multicast traffic for visiting clients.

- To use proxy Mobile IP with DHCP-enabled client devices, you must disable Media Sense on the client devices. You can find instructions for disabling Media Sense in *Microsoft Knowledge Base Article Q239924*. Click this URL to browse to this article:
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q239924&>
- Proxy Mobile IP does not support VLANs.
- If you disable proxy Mobile IP on your access point, the entire proxy Mobile IP configuration is cleared. To disable proxy Mobile IP without clearing the configuration, use the **ip proxy-mobile pause** command.

Configuring Proxy Mobile IP on Your Wired LAN

Proxy Mobile IP on access points works in conjunction with Mobile IP configured on your network routers. For instructions on configuring Mobile IP on a router on your network, refer to the Mobile IP chapter in *12.2 T New Features (Early Deployment Releases)*. Click this link to browse to the Mobile IP chapter:

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



Note

To avoid problems with roaming client devices, you must configure two hidden global configuration mode commands on your Mobile IP router: **ip mobile bindupdate** and **ip mobile bindupdate ack**.

Configuring Proxy Mobile IP on Your Access Point

Beginning in privileged EXEC mode, follow these steps to configure proxy Mobile IP on your access point:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip proxy-mobile enable	Enable proxy Mobile IP on the access point.
Step 3	ip proxy-mobile aap <i>ip-address</i> <i>[ip-address]</i> <i>[ip-address]</i>	Designate the access points that serve as the authoritative access points (the access points with which this access point compares its subnet table). Note You should specify at least two access points as AAPs in case one AAP fails. If you designate only one AAP and it goes offline, you lose all the information in the subnet map table.

	Command	Purpose
Step 4	ip proxy-mobile secure node <i>address-start address-end</i> spi <i>spi</i> key { <i>hex ascii</i> } <i>key</i>	Create security association settings for an IP address or for a range of IP addresses. <ul style="list-style-type: none"> Enter an IP address, or the starting and ending addresses in an IP range. Enter the security parameter index. Enter a key for the security parameter. Specify whether the key contains hexadecimal or ASCII characters. If you choose hexadecimal, the key must contain 32 characters. If you choose ASCII, the key can contain up to 16 characters with no minimum length.
Step 5	interface fastethernet 0	Enter interface configuration mode for the Ethernet port.
Step 6	ip proxy-mobile	Enable proxy Mobile IP on the Ethernet port.
Step 7	exit	Return to global config mode.
Step 8	interface dot11radio { 0 1 }	Enter interface configuration mode for the radio port. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 9	ip proxy-mobile	Enable proxy Mobile IP on the radio port.
Step 10	ssid <i>ssid</i>	Enter an SSID for which you want to enable proxy Mobile IP. Note Proxy Mobile IP functionality is not supported on SSIDs where VLAN is also enabled.
Step 11	ip proxy-mobile	Enable proxy Mobile IP for the SSID.
Step 12	exit	Return to global config mode.
Step 13	interface bvi1	Enter interface configuration mode for the bridge virtual interface (BVI).
Step 14	ip proxy-mobile	Enable proxy Mobile IP on the BVI.
Step 15	end	Return to privileged EXEC mode.
Step 16	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the **ip proxy-mobile** commands to disable proxy Mobile IP. Use the **ip proxy-mobile pause** command to disable proxy Mobile IP without losing your proxy Mobile IP configuration.

This example shows how to enable proxy Mobile IP on an access point for the SSID *tsunami* for IP addresses from 10.91.7.151 to 10.91.7.176:

```
ap1200# configure terminal
ap1200(config)# ip proxy-mobile enable
ap1200(config)# ip proxy-mobile aap 192.168.15.22 192.168.15.24 192.168.15.28
ap1200(config)# ip proxy-mobile secure node 10.91.7.151 10.91.7.176 spi 102 key ascii
0987654
ap1200(config)# interface fastethernet 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# interface dot11radio 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# ssid tsunami
ap1200(config-if-ssid)# ip proxy-mobile
ap1200(config-if-ssid)# exit
ap1200(config-if)# exit
ap1200(config)# interface bvi1
ap1200(config-if)# ip proxy-mobile
ap1200(config-if-ssid)# end
```