



Configuring Proxy Mobile IP

This chapter describes how to enable and configure your access point's proxy Mobile IP feature. The chapter contains the following sections:

- [Proxy Mobile IP, page 6-2](#)
- [The Proxy Mobile IP Setup Page, page 6-11](#)
- [Configuring Proxy Mobile IP, page 6-18](#)

Proxy Mobile IP

These sections explain how access points conduct proxy Mobile IP:



Note

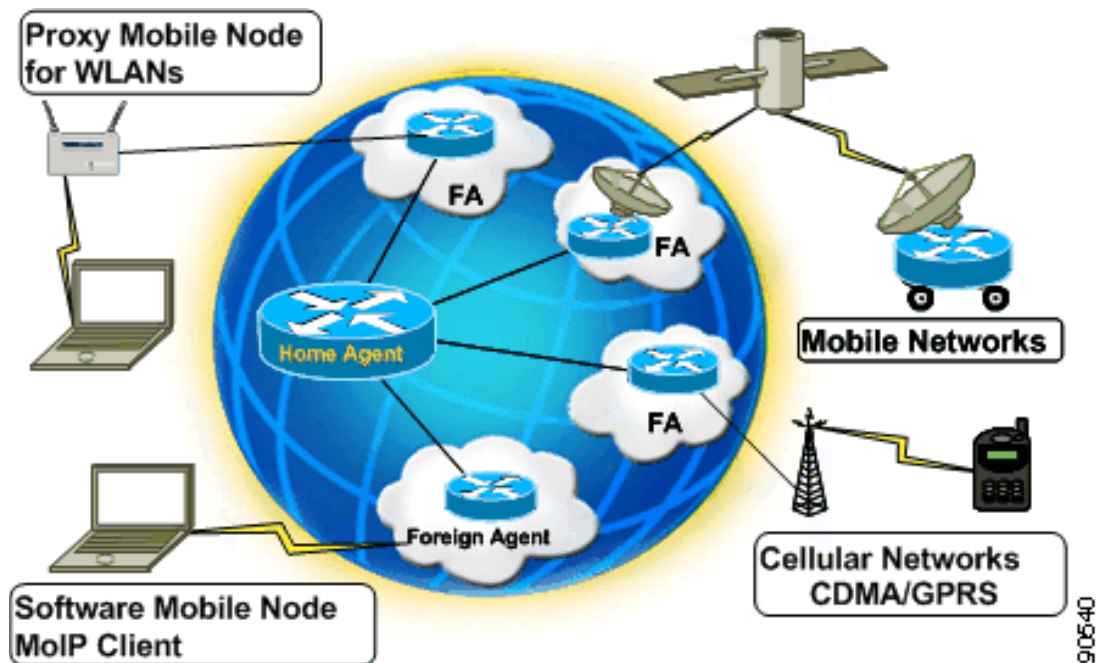
Additional information can be found in the *Proxy Mobile IP Deployment Guide*, which is available on Cisco.com.

Introduction to Mobility in IP

The advent of wireless technologies such as IEEE 802.11b has presented a tremendous opportunity to those who rely on networking resources. Devices such as laptops or handheld computers are no longer restricted to access provided by Ethernet wiring or telephone lines. As the reach of wireless coverage expands beyond the campus to metropolitan, national, and global levels, maintaining connectivity with a client's parent, or *home* network becomes more viable and expected.

Various approaches exist to providing network access to devices or *nodes* that have roamed away from their home network and onto a *foreign* network as shown in Figure 6-1. In some cases, the foreign network may be owned or administrated by a different entity such as a police or fire department. In other cases, the foreign network may simply be another Layer 3 subnet at a remote facility of a large enterprise or university campus.

Figure 6-1 The Varied Approach to Mobility



The Nomadic Approach

A nomadic node is a device that moves, or roams from one network to another. In order to use that network, the device must renew its IP address and re-establish connectivity to any applications that were in progress. There are advantages and disadvantages to the nomadic approach.

ISPs treat all devices as nomads. This means that any device requiring connectivity must request an IP address through DHCP and be assigned a routable address that falls within the range assigned to that service provider. After an address is assigned, the user can connect to the Internet and perhaps run a Virtual Private Network (VPN) on top of the connection to obtain secured access to private networks. Although this scheme provides mobility in the sense that a user can move from place to place and connect to a public network, it does not maintain any sessions that are in progress. Also, the user is aware that a change in network service has occurred.

The advantage to being a nomad is that service is available at a number of locations from a number of providers. A disadvantage is that the process of connecting to that network is manual and sometimes cumbersome. In addition, many applications do not run well when an IP address changes or a lengthy connectivity timeout occurs.

The Mobile Approach

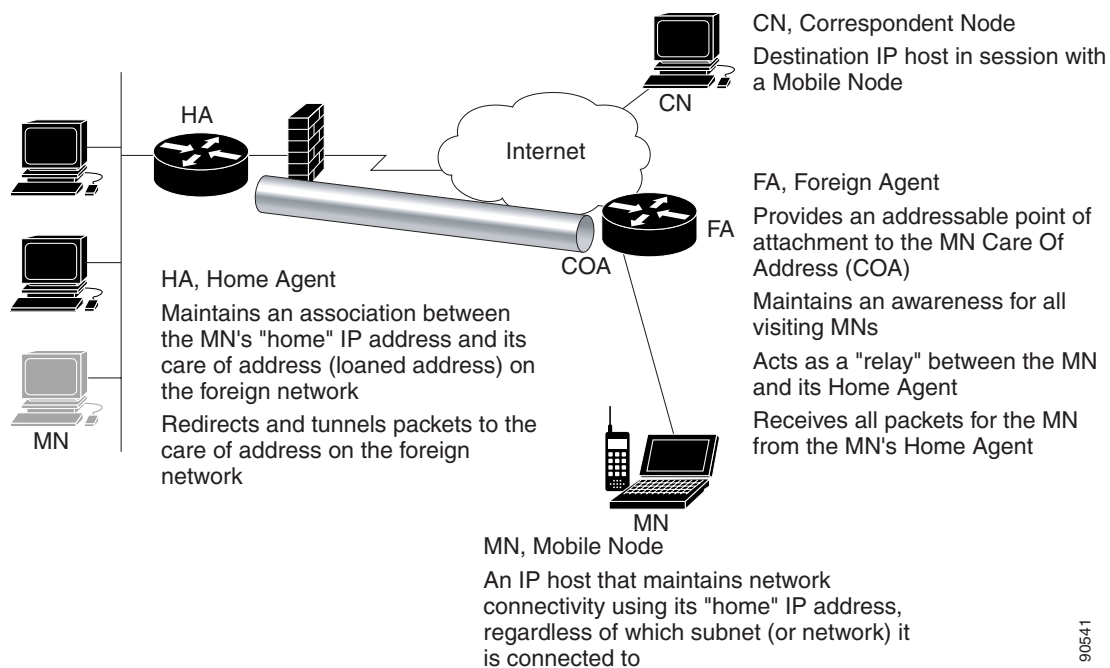
In contrast, a mobile node is a device that moves from one network to another while keeping its original IP address. This arrangement has an additional advantage of having many applications continue uninterrupted as long as the brief delay involved in roaming does not prompt a disconnect.

The major advantage of being a mobile node is that the device can now cross Layer 3 boundaries and, through a tunnel back to the a router on its home network, have its traffic forwarded to it. This tunnel back allows the device to keep its original IP address even though that address is no longer valid for the subnet to which it has roamed.

Mobile IP Explained

A clear understanding of proxy Mobile IP requires a foundation knowledge of Mobile IP. [Figure 6-2](#) identifies the components and explains the terminology used in Mobile IP.

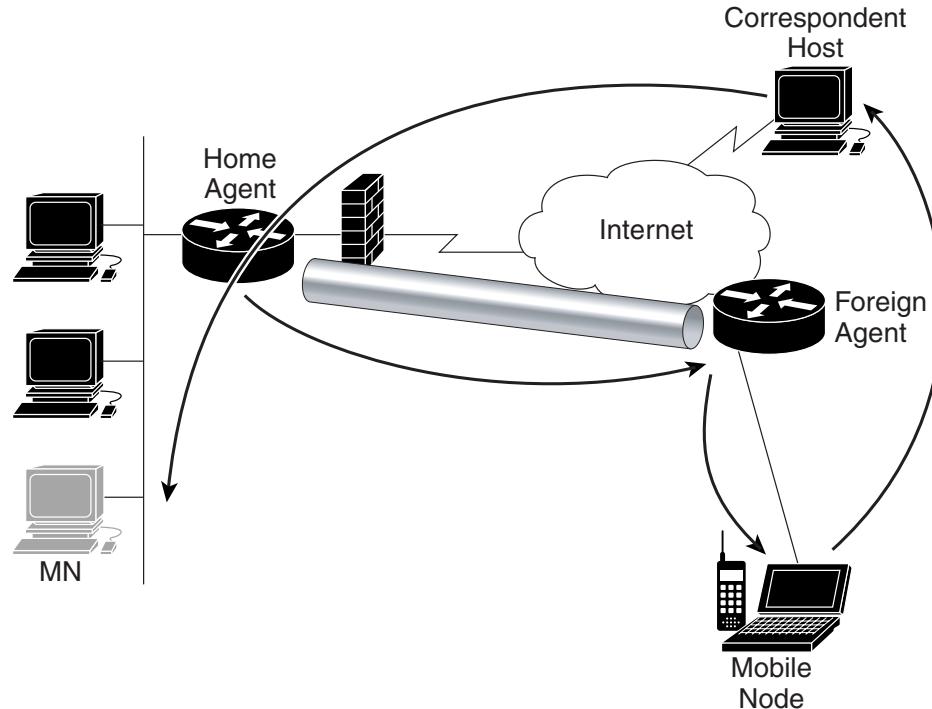
Figure 6-2 The Mobile IP Environment



In order for a mobile node (MN) to successfully roam across subnets it must first be anchored to its home network. The home agent (HA) is the router that serves as that anchor. The home agent contains a list of all devices (by IP address) that are capable of roaming from its network. After the mobile node roams to a new network, it must register with the home agent as being away from home. Its registration is sent by way of the Foreign Agent (FA), the router providing service on the foreign network. The foreign agent includes a *care-of address* in the registration it sends to the home agent. This address is used as the termination address of the tunnel on the foreign router. A tunnel is then built between the home agent and the foreign agent for all traffic destined for the mobile node.

When a mobile node sends traffic to another device (known as a *correspondence node* or *correspondence host*), such as a web server, the outbound traffic is routed directly to the destination device. The destination device replies to the source IP address, resulting in the traffic being routed to the home agent because it is the default router for the subnet from which the mobile node originated. The home agent then forwards the traffic through the tunnel to the foreign agent, which forwards it to the mobile node. Figure 6-3 provides an example of this process.

Figure 6-3 The Mobile IP Traffic Pattern



- Traffic is sent from the MN directly to the Correspondent Host
- The Host replies to the source address of the MN
- The traffic is routed to the HA
- The HA tunnels the traffic to the CoA of the FA
- The FA forwards the traffic to the MN

90542

When the mobile node roams back to its home network, it drops its registration with the home agent and the tunnel is removed. If more than one node has roamed from the same home network to the same foreign network, a single tunnel is used to service traffic for all mobile devices between those two tunnel end points.

The protocol used to exchange information between the home agent and mobile node is the Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP). Extensions have been added to this protocol to accommodate Mobile IP operation. Mobile IP features on a Cisco router require the IP Plus Feature Set or better.

Proxy Mobile IP Explained

The Mobile IP operation detailed above relies upon the mobile node using specialized Mobile IP client software. This software provides the intelligence needed to communicate with other Mobile IP entities such as home and foreign agents, plus the ability to generate registrations as appropriate. However, there are a few aspects of this method that make it undesirable. They include the cost of client software, the amount of administration required to load it onto some (potentially large) number of devices, and the possibility that the population of mobile nodes may not be immediately known or may change over time.

Proxy Mobile IP supports Mobile IP for wireless nodes without requiring specialized software for those devices. The wireless access point acts as a proxy on behalf of wireless clients that are not aware of the fact that they have roamed onto a different Layer 3 network. The access point handles the IRDP communications to the foreign agent and handles registrations to the home agent. This scheme offers less cost, less administration, and a faster time to deployment.

There are three primary states of operation for proxy Mobile IP:

- Agent discovery
- Updating the subnet map table
- Device registration

The following paragraphs offer a high-level view of how proxy Mobile IP operates.

The IRDP handles agent discovery in proxy Mobile IP. This protocol must be enabled on the home agent and foreign agent router interfaces on which access points reside. The protocol enables the access point to identify services being offered by local Mobile IP entities and provides some necessary information to be used when an access point must register a mobile node.

Any access point in the network may be designated as an authoritative access Point (AAP), which means that it updates all other access points in the network about networks that have mobile nodes on them. The protocol used for this interaction is UDP-based (port 6500) and is enabled when proxy Mobile IP is enabled.

An access point that has discovered a foreign agent on its network and has received an updated subnet map from the authoritative access point is ready to service mobile nodes, which roam to it from other subnets. The mobile node decides to roam to a new access point based on criteria such as signal strength, traffic load on the access point, and so forth. Once associated, the mobile node eventually sends traffic to the access point. The access point recognizes that the source address in use is from a different Layer 3 network than its own and checks its subnet map table for an entry. If the subnet matches one of the entries in the table, the access point sends a registration request to the local foreign agent requesting that the mobile node be registered with the proper home agent. The foreign agent in turn forwards the registration request to the home agent.

The home agent verifies that the mobile node is valid (either through its local security associations or through associations housed on a AAA server). If it is valid, the home agent binds the mobile node to the foreign agent's care-of address and builds a tunnel between the foreign agent and the home agent. Traffic can then flow from the home agent to foreign agent, from foreign agent to access point, and from access point to mobile node. The mobile node can send traffic to directly to the node to which it is intended.

Before Deploying Proxy Mobile IP

Before deploying proxy Mobile IP, you should ask some fundamental questions of the network design and implementation engineers:

- Is there an alternative to using proxy Mobile IP?
- What is the corporate policy regarding device roaming?
- Should you use static or dynamic IP address assignments?
- Do I have an operational Mobile IP network or do I need to build one from scratch?
- If I build a network from scratch, do I have the right software revision and feature set on my routers?

The answers to these questions may vary. For further information, see the *Proxy Mobile IP Deployment Guide*.

Issues to Consider While Deploying Proxy Mobile IP

When deploying proxy Mobile IP, consider these key issues:

- Proxy Mobile IP is currently not supported with VLANs. Do not enable VLANs if you plan to use proxy Mobile IP.
- Enabling proxy Mobile IP on the access point requires software release 12.01T1 or later.
- Synchronize clocks between access points, home agents, and foreign agents and use the Network Time Protocol (NTP) rather than manually setting clocks. Registration requests may fail if the timestamps generated by the requestor are outside the window expected by the receiver.
- Be sure to enable proxy Mobile IP on each SSID that requires it. None of the proxy Mobile IP configuration commands take effect until proxy Mobile IP is set on the SSID.
- An access point providing proxy Mobile IP must have a default gateway assigned (statically or through DHCP).
- A home agent or foreign agent must be running on the network's default gateway (assuming there are multiple routers on the subnet). If both home and foreign agents exist on a single subnet, they must be configured on the same gateway.
- In networked environments where mobile nodes reside on multiple subnets, routers providing proxy Mobile IP services may need to act as both a home agent (for local subnets) and a foreign agent (for remote subnets). Commands that enable these features can be applied to the same router without interfering with each other.
- Proxy Mobile IP does not support broadcast or multicast capabilities for the roaming client device. Applications that rely on multicast should not be enabled as proxy Mobile IP clients.
- Verify that there is IP connectivity between all devices before attempting to troubleshoot a proxy Mobile IP problem. Ping all devices and interfaces in the network that perform proxy Mobile IP functions.
- Use loopback interfaces for any function that requires an IP address but does not require a specific interface, such as care-of address on the foreign agent.
- Make sure that UDP port 6500 is not blocked between the authoritative access point and other access points. A blockage prevents the propagation of subnet table updates.

Components of a Proxy Mobile IP Network

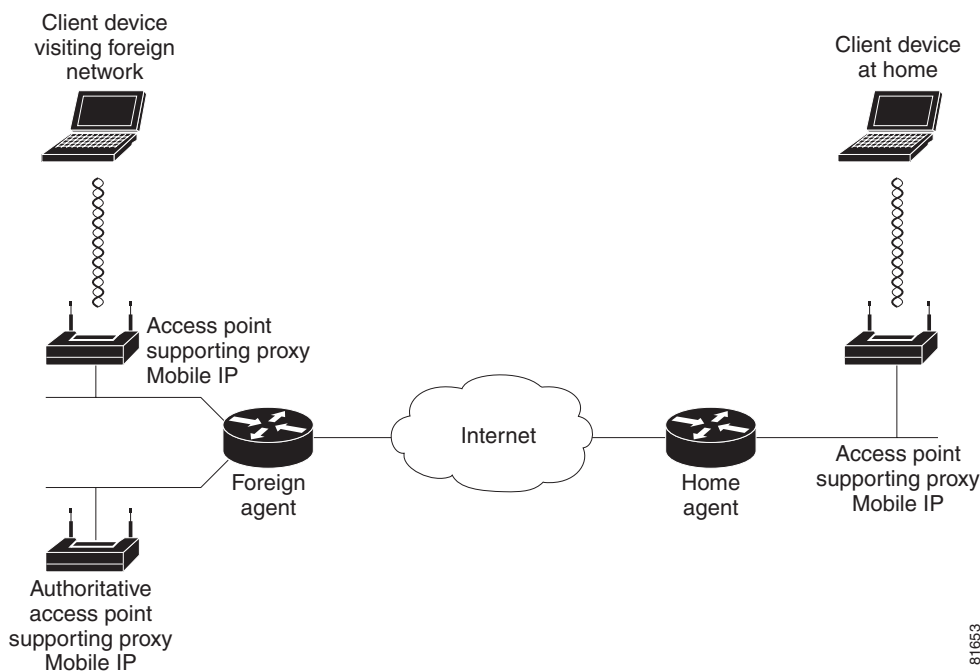
Five devices participate in proxy Mobile IP:

- 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 Mobile IP client software.
- An access point with proxy Mobile IP enabled. The access point proxies on behalf of the visiting client device, performing all Mobile IP functions for the device. The access point uses a subnet map to keep track of home agent information. The access point also gets updates about new home agents from the authoritative access point.
- An authoritative access point on your network supporting proxy Mobile IP. The authoritative access point uses a subnet map to collect and distribute home agent information stored in the subnet map to all the other access points 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 by way of a tunnel to a foreign agent.
- 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 6-4 shows the five participating devices.

Figure 6-4 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 6-8](#)
- [Subnet Map Exchange, page 6-9](#)
- [Registration, page 6-10](#)
- [Tunneling, page 6-10](#)

Agent Discovery

During the agent discovery phase, the home agent and the foreign agent advertise their services on the network by using the IRDP. The access point monitors 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 must have the home agent IP address of the visiting client, which it gets from 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 6-1](#) is an example of a subnet map table.

Table 6-1 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 can be any access point on the network that the network administrator chooses. The AAP is responsible for maintaining 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 an invalid registration packet with a bad SPI and group key using the broadcast address of the home agent subnet to determine 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 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.

As an access point on a network with a local home agent, the access point registers mobile nodes with the home agent prior to any roaming taking place. Mobile nodes must be listed by IP address (or address range) in the access point and the home agent along with security information stored either locally, on a AAA server, or both.

On the foreign network, 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 verifying 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 access point hosting the visiting client through the foreign agent (because the registration request was received through the foreign agent). The foreign agent verifies 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 reregisters 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 reregistration.

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.

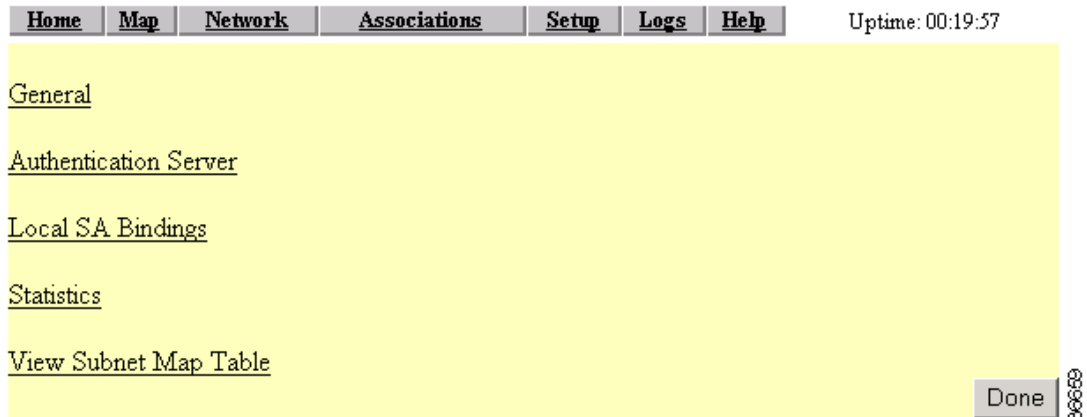
Optionally, the mobile-foreign authentication extension and the foreign-home authentication extension are appended to protect message exchanges between a visiting client and foreign agent and between a foreign agent and home agent, respectively.

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. If the timestamp in the first registration request is out of the tolerance window (± 7 seconds), the request is rejected. The access point uses the information from the rejection to create a valid value and resends the registration request.

The Proxy Mobile IP Setup Page

This section describes the Proxy Mobile IP Setup page and the links it provides to other pages you use to set up proxy Mobile IP on your access point. [Figure 6-5](#) shows the Proxy Mobile IP Setup page.

Figure 6-5 Proxy Mobile IP Setup page



Follow this link path to reach the Proxy Mobile IP Setup page:

1. On the Summary Status page, click **Setup**.
2. In the Services section of the Setup page, click **Proxy Mobile IP**.

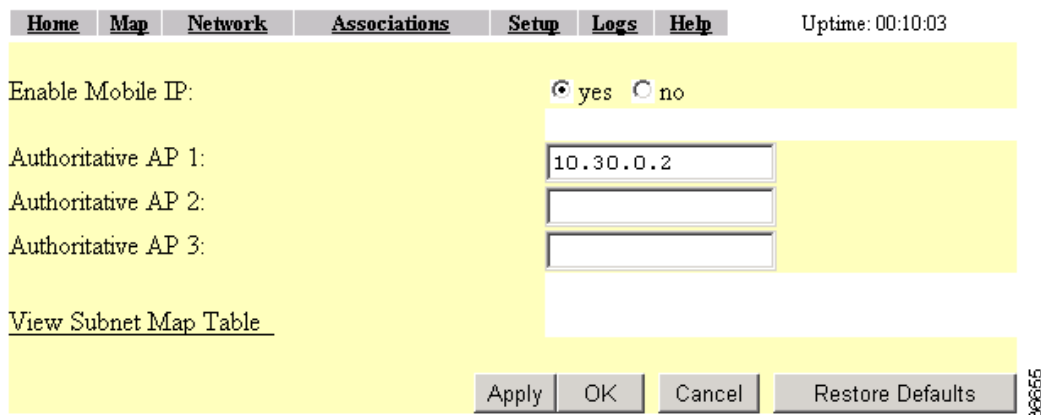
There are 5 links on the page:

- [General](#)
- [Authentication Server](#)
- [Local SA Bindings](#)
- [Statistics](#)
- [View Subnet Map Table](#)

General

Selecting the **General** link takes you to the Proxy Mobile IP General page (Figure 6-6), where you enable proxy Mobile IP on the access point and identify the IP addresses of the authoritative access points on your wireless network.

Figure 6-6 Proxy Mobile IP General Page



Settings on the Proxy Mobile IP General Page

Enable Proxy Mobile IP

This setting enables the proxy Mobile IP feature on the access point. The default setting is **no**.



Note

Proxy Mobile IP must also be enabled for the SSID you intend to use to support the feature. Otherwise, proxy Mobile IP will not work. See the “[Configuring Proxy Mobile IP](#)” section on page 6-18 for additional information.

Authoritative AP *n*

These settings identify the IP addresses of up to three AAPs on the wireless network. At least one AAP is required for the proxy Mobile IP enabled wireless network. The *n* represents the number of the authoritative access point. Among other tasks, the authoritative access point is the device that registers with the local home agent. After registering with the home agent, the AAP populates a subnet map that is distributed to other access points. The subnet map links the access points to the home agent to contact and register a mobile client based on the client’s IP address. For example, if a mobile client appears with a “30” subnet IP address on the “20” subnet, the access point must register with the home agent that services subnet “30” mobile clients.

Authentication Server

Selecting the Authentication Server link takes you to the Authenticator Configuration page (Figure 6-7). From this page, you configure the RADIUS or TACACS servers that will be managing proxy Mobile IP wireless devices.

Figure 6-7 Authenticator Configuration Page

[Map](#) [Help](#)
Uptime: 1 day, 19:55:08

802.1X Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
<input style="width: 90%;" type="text"/>	RADIUS	1812	<input style="width: 90%;" type="text"/>	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
<input style="width: 90%;" type="text"/>	RADIUS	1812	<input style="width: 90%;" type="text"/>	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
<input style="width: 90%;" type="text"/>	RADIUS	1812	<input style="width: 90%;" type="text"/>	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
<input style="width: 90%;" type="text"/>	RADIUS	1812	<input style="width: 90%;" type="text"/>	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					

Note: For each authentication function, the most recently used server is shown in green text.

Apply
OK
Cancel
Restore Defaults

65555

Settings on the Authenticator Configuration Page

802.1X Protocol Version (for EAP Authentication)

This drop-down menu allows you to select the draft of the 802.1X protocol the access point's radio will use. EAP operates only when the radio firmware on client devices complies with the same 802.1X Protocol draft as the management firmware on the access point. See the [“Setting Up EAP Authentication” section on page 8-15](#) for additional information.

Primary Server Reattempt Period (Min)

This field specifies how many minutes should pass before checking for the primary server when it was not initially accessible.

Server Name/IP

This field identifies the domain name or IP address of the RADIUS or TACACS server proxy Mobile IP is using for authentication purposes.

Server Type

This drop-down menu displays the selections you can make to designate the server type you want the proxy Mobile IP configuration to use. The choices are RADIUS or TACACS. RADIUS is the default setting.

Port

This field specifies the port number the server uses for authentication. The default setting, 1812, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server, and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.

Shared Secret

This field identifies the shared secret used by your RADIUS server. The shared secret on the access point must match the shared secret on the RADIUS server. The shared secret can contain up to 64 alphanumeric characters. This setting has no default.

Retran Int (sec)

This field specifies the time interval in seconds that the server waits after it failed to contact the server until it tries again. The default setting is 5 seconds.

Max Retran

This field indicates how many times the server attempts to contact the server before it attempts to contact an alternate server. The setting works in conjunction with the Retran Int (sec) parameter.

Use server for:

These check boxes specify the authentication types the server uses: EAP, MAC Address, User, or MIP authentication. Checking the EAP authentication check box designates the server as an authenticator for any EAP type, including LEAP, PEAP, EAP-TLS, LEAP-SIM, and EAP-MD5. Checking the MIP authentication configures the server to authenticate proxy Mobile IP configured clients.

Local SA Bindings

Selecting the Local SA Bindings link takes you to the Local SA Bindings page (Figure 6-8). You use this page to identify valid clients that are able to establish contact with a foreign agent in another network segment or network other than the client's home network.

Figure 6-8 Local SA Bindings Page

Home Map Network Associations Setup Logs Help 2002/11/26 03:13:55

New SA Binding:

IP Address Range - Start: Add

IP Address Range - End:

Group SPI:

Group Key:

Enter 32-bit SPI as 8 hexadecimal digits (0-9, a-f, or A-F) with range (100-FFFFFFF).
Enter 128-bit Key as 32 hexadecimal digits (0-9, a-f, or A-F).

Existing SA Bindings: Remove

10.30.0.20	10.30.0.25	100	14141414141414141414141414141414
10.30.0.26	10.30.0.27	100	14141414141414141414141414141414

Apply OK Cancel Restore Defaults 88867

Settings on the Local SA Bindings Page

IP Address Range - Start

This field contains the beginning IP address of the range in which client devices must reside in order to be valid.

IP Address Range - End

This field contains the ending IP address of the range in which the client devices must reside in order to be valid.

Group SPI

This field specifies the security parameter index of the IP address range entered in the IP Address Range - Start and End fields. The SPI is a 32-bit number (8 hexadecimal digits) assigned to the initiator of the security association request by the receiving IPsec endpoint. On receiving a packet, the destination address, protocol, and SPI are used to determine the security association. The security association allows the node to authenticate or decrypt the packet according to the security policy configured for that security association.

Group Key

This field contains an authentication key, similar to a WEP key, that the group specified in the security association uses to access a foreign agent. The group key is a 128-bit key entered as 32 hexadecimal digits (0-9, a-f, or A-F).

Existing SA Bindings

This field contains a listing of previously configured security association bindings. The information contains the beginning and ending IP address range and their associated group SPI and key settings.

Statistics

Selecting the Statistics link takes you to the Proxy Mobile IP Statistics page (Figure 6-9). Two buttons are available on this page:

- Refresh—Click this button to refresh the data on the screen.
- Clear—Click this button to clear the data on the screen and begin a new round of data collection.

Figure 6-9 Proxy Mobile IP Statistics Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 01:12:57
Mobile IP Status : Enabled							
Home Agents : Not found							
Foreign Agents : Not found							
Active AAP : 10.0.0.1							
MN IP Addresses :							
Solicitations Sent	119472	Registration Request Successes	0				
Authentication Failures for HA	0	Authentication Failures for FA	0				
Registration Requests Sent	0	Deregister Requests Sent	0				
Registration Replies Received	0	Deregister Replies Received	0				
Registration Requests Denied by FA	0	Registration Requests Denied by HA	0				
Advertisements Received	0	Gratuitous ARPs sent	0				

Settings on the Proxy Mobile IP Statistics Page

Mobile IP Status

This informational field indicates whether proxy Mobile IP is enabled or disabled.

Home Agents

This informational field provides information about home agents the access point discovers on its own subnet. If a home agent is discovered, its IP address is displayed. If multiple home agents are discovered, their IP addresses are displayed. If no agent is discovered, the field displays Not Found.

Foreign Agents

This informational field provides information about foreign agents it discovers on the access point discovers on the network. If a foreign agent is discovered, its IP address is displayed. If multiple foreign agents are discovered, their IP addresses are displayed. If no agent is discovered, the field displays Not Found.

Active AAP

This informational field lists the IP address of the active authoritative access point.

MN IP Addresses

This informational field lists the IP addresses of the mobile nodes, which are client devices that the access point is servicing.

Solicitations Sent

The number of agent solicitations messages the access point has sent. If the access point does not hear advertisements, it sends a solicitation message requesting a foreign or home agent acknowledgement. The solicitation forces any agents on the link to immediately send an agent advertisement.

Authentication Failures for HA

The number of times the home agent rejected registration requests because of authentication failures, such as an invalid SPI or group key. When a mobile node moves to a foreign network, the access point registers the mobile node to its home agent. This statistic indicates the number of registration failures caused by failure of the home agent or foreign agent to authenticate each other or the mobile node.

Registration Requests Sent

The number of registration requests sent by the access point for the mobile node.

Registration Request Denied by FA

The number of times a foreign agent rejected a registration request. When a mobile node moves to a foreign network, the access point registers the mobile node to its home agent. This statistic indicates the number of registration requests that were denied by the foreign agent. The reasons for denial vary and include home agent unreachable, no resources found, etc.

Advertisements Received

The number of IRDP advertisements received by agents.

Registration Requests Successes

The number of times registration requests were successful.

Authentication Failures for FA

The number of times the foreign agent rejected registration requests because of mobile node or home agent authentication failures.

Deregister Requests Sent

The number of times the access point sent deregistration requests to the home agent.

Deregister Replies Received

The number of times the access point received deregistration replies from the home agent.

Registration Requests Denied by HA

The number of times the home agent rejected registration requests.

Gratuitious ARPs sent

The number of times the access point sent gratuitous Address Resolution Protocol messages (ARPs). Gratuitous ARPs are sent by the home agent on behalf of a roaming mobile node to update the ARP caches on the local hosts. When the mobile node returns to its home network, the home access point sends gratuitous ARPs (on behalf of the mobile node) to notify the network of the mobile node's MAC and IP address.

View Subnet Map Table

Selecting the View Subnet Map Table link takes you to the Subnet Map Table page (Figure 6-10). The subnet map table contains a list of home agent IP addresses and their associated subnet masks.

Two buttons are available on this page that are not shown on Figure 6-10:

- Clear—removes entries from the table that are no longer valid
- Refresh—validates and renews entries on the table

Figure 6-10 Subnet Map Table Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:30:19
HA Address		Subnet Mask					
10.30.0.1		255.255.255.0					
10.20.0.1		255.255.255.0					

Settings on the Subnet Map Table Page

HA Address

This column lists the IP addresses of the home agents.

Subnet Mask

This column lists the subnet mask addresses for the corresponding home agents.

Configuring Proxy Mobile IP

Proxy Mobile IP functions as a proxy on behalf of roaming clients that do not implement a Mobile IP software stack. In a Mobile IP environment, the access point uses the services of a home agent and a foreign agent to allow valid mobile nodes to access a working Mobile IP network on a wired LAN. A working Mobile IP network assumes the following:

- At least one router in the network functions as a home agent where mobile clients will be based.
- At least one router in the network functions as a foreign agent, to which mobile clients will roam.

- Access points configured as authoritative access points must be enabled for proxy Mobile IP before regular access points.
- All proxy Mobile IP enabled access points in the network must be configured to use the same authoritative access points. For example, one access point cannot be configured with two authoritative access points and another access point be configured with three different authoritative access points.

Optionally, you can implement an AAA server to authenticate mobile clients in addition to home and foreign agents.

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>

In addition, make sure you have accomplished the following actions:

- Loaded the latest firmware onto all access points in your wireless network.
- Established an HTTP connection to the access point.
- Verified that client devices are associated to the local access point.
- Verified receipt of an appropriate DHCP address for the local LAN segment.
- Confirmed IP connectivity between all devices (ping or HTTP).

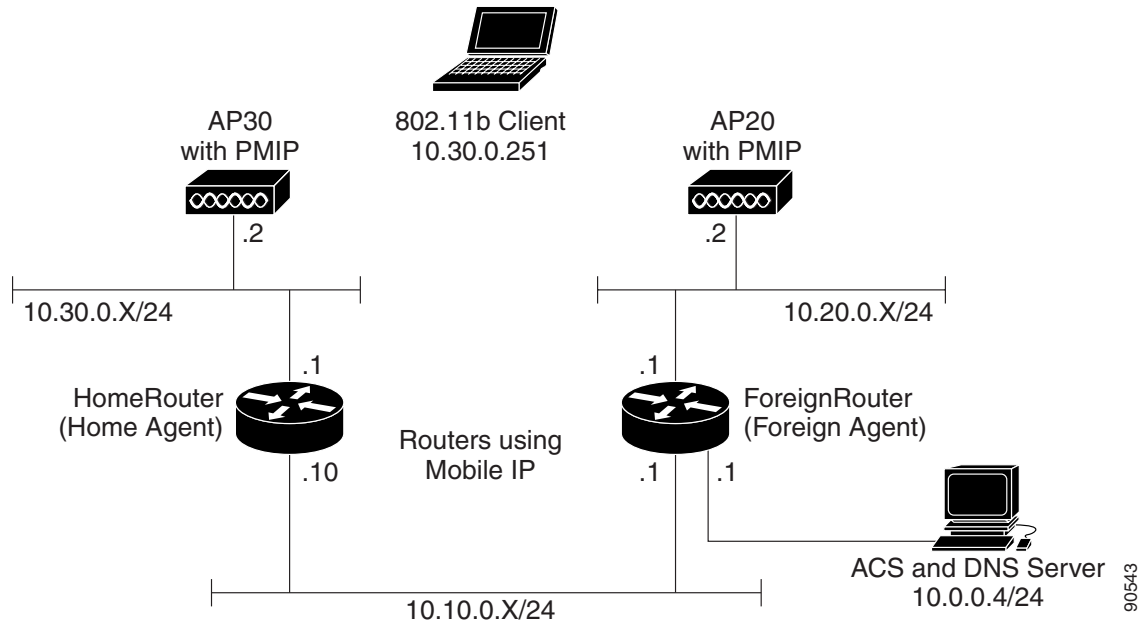
At least one access point on the wireless side of a home and foreign network must be a home or foreign agent access point. Both access points must be configured to enable valid mobile nodes to associate with them.

There are no standard procedures that describe how to configure these agent access points. Configuration parameters, such as SSIDs, valid proxy Mobile IP addresses, SPI keys and group keys, and security settings must be carefully considered and coordinated with wired side router settings before any degree of success can be expected. The basic settings are the same for both access points. The only difference is where the access point is located. A home agent access point is on the wireless side of the mobile node's home network. A foreign agent access point is on the wireless side of the network in which the mobile node is authorized to enter in order to communicate back to its home network.

These instructions provide a general overview of the steps involved to configure the wireless network components to operate in a Mobile IP environment. It must be stressed that the majority of configuration effort is devoted to components on the wired network.

Figure 6-11 shows the configuration described in the following sections.

Figure 6-11 A Sample Network



Follow these steps to create a Proxy Mobile IP configuration.

-
- Step 1** Browse to the access point's Setup page.
- Step 2** In the Associations section, click **SSIDs: Int**. The AP Radio: Internal Service Sets page appears (Figure 6-12).

Figure 6-12 AP Radio Internal SSID #x Page

The screenshot shows the 'Service Set Summary Status' page in a web browser. The page has a navigation bar with tabs: Home, Map, Network, Associations, Setup, Logs, Help. The 'Setup' tab is active. The page title is 'Service Set Summary Status' and the uptime is '7 days, 21:54:06'. The page contains the following fields and controls:

- Device:** AP Radio: Internal
- SSID for use by Infrastructure Stations (such as Repeaters):** [0]
- Disallow Infrastructure Stations on any other SSID:** yes no
- Service Set ID(SSID):** []
- Existing SSIDs:**
 - [0] Test AP 2(primary)
 - [1] bnetwork30
- Buttons:**

A vertical label '90544' is on the right side of the screenshot.

- Step 3** Select the SSID on which proxy Mobile IP will be supported and click **Edit**. The AP Radio: Internal Primary SSID page appears (Figure 6-13).

Figure 6-13 AP Radio: Internal Service Sets Page

Uptime: 4 days, 01:38:36

Map Help

Device: AP Radio: Internal

Service Set ID (SSID): bnetwork30

Current Number of Associations: 0

Maximum Number of Associations: 0

Proxy Mobile IP is enabled: yes no

Default VLAN ID: [0] -None-

Default Policy Group ID: [0] -None-

Accept Authentication Type: Open Shared Network-EAP

Require EAP:

Default Unicast Address Filter: Allowed Allowed Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults

- Step 4** Enable proxy Mobile IP for this SSID.
- Step 5** Click **OK** twice. You are returned to the Setup page.
- Step 6** In the Services section, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears (Figure 6-14).

Figure 6-14 Proxy Mobile IP Setup Page

Home Map Network Associations Setup Logs Help Uptime: 00:19:57

General

Authentication Server

Local SA Bindings

Statistics

View Subnet Map Table

Done

- Step 7** Click **General**. The Proxy Mobile IP General page appears (Figure 6-15).

Figure 6-15 Proxy Mobile IP General Page

Home Map Network Associations Setup Logs Help Uptime: 7 days, 22:18:51

Enable Proxy Mobile IP: yes no

Authoritative AP 1:

Authoritative AP 2:

Authoritative AP 3:

Apply OK Cancel Restore Defaults

- Step 8** Set the Enable Proxy Mobile IP setting to **yes**.
- Step 9** Enter the IP address of the access point in the Authoritative AP 1 field.
- Step 10** Click **OK**. You are returned to the Proxy Mobile IP Setup page.
- Step 11** If you are using a CiscoSecure ACS server for security associations, go to the [“Configuring Mobile IP Security Associations on a CiscoSecure ACS Server”](#) section on page 6-23
- Step 12** From the Proxy Mobile IP Setup page, select **Local SA Bindings**. The Local SA Bindings page appears (Figure 6-17).

Figure 6-16 Local SA Bindings Page

Home Map Network Associations Setup Logs Help Uptime: 7 days, 22:29:36

New SA Binding:

IP Address Range - Start: Add

IP Address Range - End:

Group SPI:

Group Key:

Enter 32-bit SPI as 8 hexadecimal digits (0-9, a-f, or A-F) with range (100-FFFFFFFF).
Enter 128-bit Key as 32 hexadecimal digits (0-9, a-f, or A-F).

Existing SA Bindings: Remove

Apply OK Cancel Restore Defaults

- Step 13** Add the entries for a specific host or a range of IP addresses of mobile nodes, along with a Group SPI and Group Key.
- Step 14** Click **OK**. You are returned to the Proxy Mobile IP Setup page.

- Step 15** Click **View Subnet Map Table**. The access point sees the home agent if an entry exists for the desired subnet and displays it on the Subnet Map Table page (Figure 6-17).

Figure 6-17 Subnet Map Table

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 00:30:19
HA Address		Subnet Mask					
10.30.0.1		255.255.255.0					
10.20.0.1		255.255.255.0					

- Step 16** Check the IP addresses in the HA Address column. The home agent's IP address should appear in this column.
- Step 17** Return to the Proxy Mobile IP Setup Page and click **Statistics**. The Proxy Mobile IP Statistics page appears. Check to see that the following statistics are shown:
- For access points on home networks, confirm that the home agent is listed.
 - For access points on foreign networks, confirm that the foreign agent is listed.
 - Confirm that the authoritative access point is listed on all Proxy Mobile IP-enabled access points.



Note Devices that are registered to roam are listed on the home agent access point. If a node has roamed onto a foreign access point, it should be listed in the Mobile Node IP Address section of the statistics page.

Configuring Mobile IP Security Associations on a CiscoSecure ACS Server

Follow these steps to configure the server:

- Step 1** Browse to the Proxy Mobile IP Setup page and select **Authentication Server**. The Authenticator Configuration page appears (Figure 6-18).

Figure 6-18 Authenticator Configuration Page

Map Help Uptime: 8 days, 00:34:48

802.1X Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
10.0.0.2	RADIUS	1812	XXXXXXXXXX	5	3
	RADIUS	1812	XXXXXXXXXX	5	3
	RADIUS	1812	XXXXXXXXXX	5	3
	RADIUS	1812	XXXXXXXXXX	5	3

Use server for: EAP Authentication MAC Address Authentication User Authentication MIP Authentication

Use server for: EAP Authentication MAC Address Authentication User Authentication MIP Authentication

Use server for: EAP Authentication MAC Address Authentication User Authentication MIP Authentication

Use server for: EAP Authentication MAC Address Authentication User Authentication MIP Authentication

Note: For each authentication function, the most recently used server is shown in green text.

Apply OK Cancel Restore Defaults

900545

- Step 2** Perform the following:
- In the Server Name/IP field, enter the IP address or domain name of the ACS server.
 - In the Shared Secret field, enter the shared secret key used on the ACS server.
 - Check the MIP Authentication box.
- Step 3** Click **Apply** or **OK**. You are returned to the Proxy Mobile IP Setup page.
- Step 4** On the CiscoSecure ACS server, define the home agent client device (Figure 6-19).

Figure 6-19 Network Configuration Screen for a Router Client

CISCO SYSTEMS Network Configuration

Edt

AAA Client Setup For Home_Router

AAA Client IP Address: 10.10.0.10

Key: ciscokeyXXXXXXXXXX

Authenticate Using: RADIUS (Cisco IOS/PIX)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

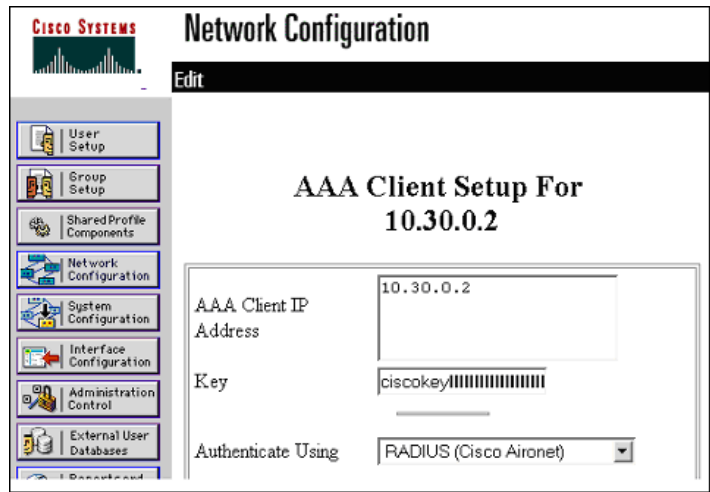
Log RADIUS Tunneling Packets from this AAA Client

User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation

900636

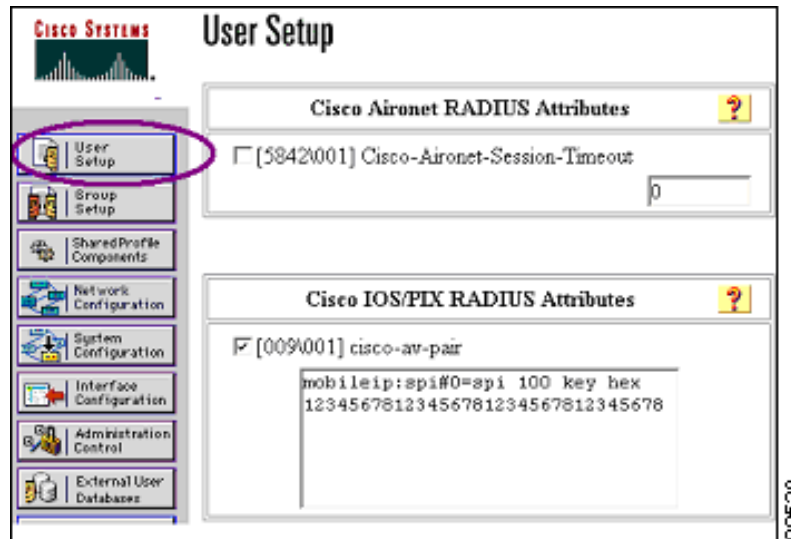
- Step 5** Define an entry for each Proxy Mobile IP-enabled access point (Figure 6-20).

Figure 6-20 Network Configuration Screen for an Access Point Client



- Step 6** Add a User entry for each mobile node (client device). Use the “cisco-av-pair” syntax as detailed in Figure 6-21.

Figure 6-21 User Setup Screen



Note If this option does not appear, enable it for the specific user or an entire group under Interface Configuration, “Radius (Cisco IOS/PIX)”, “cisco-av-pair”

- Step 7** Refer to the authentication logs and verify that all devices are communicating properly with the ACS server (Figure 6-22).

Figure 6-22 Passed Authentication Screen

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
01/14/2003	13:42:26	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:42:26	Authen OK	10.30.0.201	Default Group	000967025193	38	10.30.0.2
01/14/2003	13:42:21	Authen OK	10.30.0.201	Default Group	000967025193	38	10.30.0.2
01/14/2003	13:13:13	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:13:08	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:13:04	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:13:02	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:13:01	Authen OK	10.30.0.201	Default Group	.	10.30.0.201	10.10.0.10
01/14/2003	13:13:01	Authen OK	10.30.0.201	Default Group	000967025193	37	10.20.0.2

- Step 8** In the Services section of the Setup page, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears.
- Step 9** Click **General**. The Proxy Mobile IP General page appears.
- Step 10** Set the Enable Proxy Mobile IP radio button to **yes**.
- Step 11** Enter the IP address of the authoritative access point in the Authoritative AP 1: field.
- Step 12** Click **OK** to return to the Proxy Mobile IP Setup page.
- Step 13** Click **Local SA Bindings**. The Local SA Bindings page appears.
- Step 14** Enter the starting and ending IP addresses of the range of IP addresses designated as valid mobile node addresses.
- Step 15** Enter a predetermined SPI and Group Key in the appropriate fields.
- Step 16** Click **OK** to return to the Proxy Mobile IP Setup page.
- Step 17** Click **Done** to return to the Setup page.