



Configuring Proxy Mobile IP

This chapter describes how to enable and configure your access point's proxy Mobile IP feature.



Note

Proxy Mobile IP applies to a bridge only when configured as a root access point.

The chapter contains the following sections:

- [Proxy Mobile IP, page 6-2](#)
- [The Proxy Mobile IP Setup Page, page 6-6](#)
- [Configuring Proxy Mobile IP, page 6-14](#)

Proxy Mobile IP

These sections explain how access points conduct proxy Mobile IP:

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

Overview

The access point's proxy Mobile IP feature works in conjunction with the Mobile IP feature on Cisco devices on the wired network. 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:

- Issue a DHCP request to get a new IP address.
- 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 who use those SSIDs. Proxy Mobile IP does not support VLANs.

Proxy Mobile IP is disabled by default.

**Note**

Guest client devices do not receive broadcast and multicast packets from their home networks.

Components of a Proxy Mobile IP Network

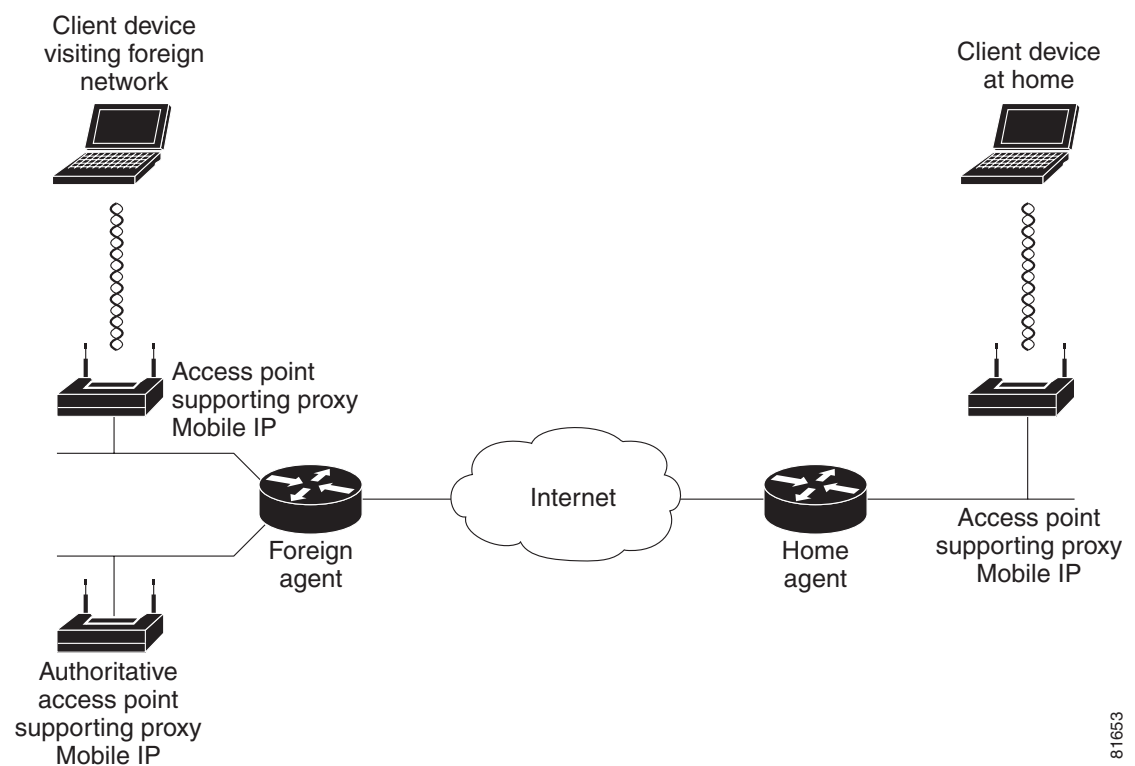
Five devices participate in proxy Mobile IP:

- 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 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 regular 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.
- 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 6-1 shows the five participating devices.

Figure 6-1 Participating Devices in Proxy Mobile IP



81653

How Proxy Mobile IP Works

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

- [Agent Discovery, page 6-4](#)
- [Subnet Map Exchange, page 6-4](#)
- [Registration, page 6-5](#)
- [Tunneling, page 6-6](#)

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 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 is an access point that maintains 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 (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 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 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.

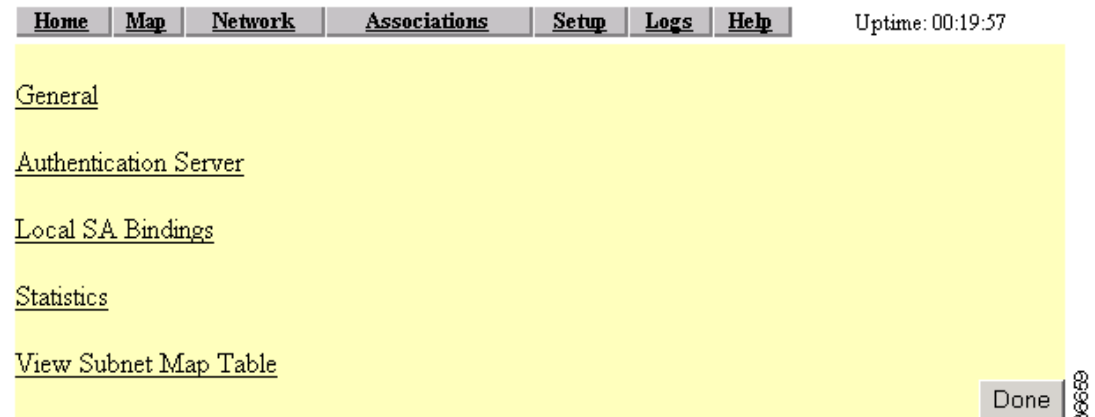
Optionally, the mobile-foreign authentication extension and the foreign-home authentication extension are appended to protect message exchanges between a visiting client and foreign agent and between a foreign agent and home agent, respectively.

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 6-2](#) shows the Proxy Mobile IP Setup page.

Figure 6-2 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**.

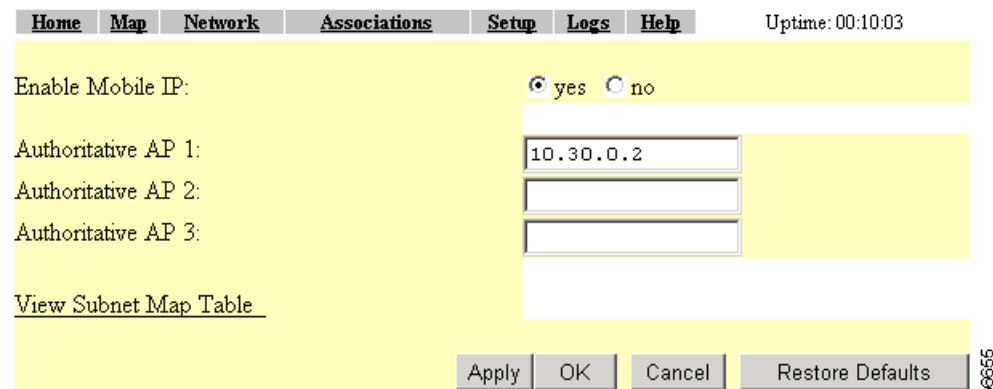
There are 5 links on the page:

- [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 6-3), 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 6-3 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 the Authoritative Access Point](#)” section on [page 6-15](#) for additional information.

Authoritative AP *n*

These settings identify the IP addresses of up to three authoritative access points (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. The authoritative access point is the device that registers with the home agent. After registering with the home agent, the AAP populates a subnet map for 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 6-4](#)). From this page, you configure the RADIUS or TACACS servers that will be managing proxy Mobile IP wireless devices.

Figure 6-4 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 |
|---|-------------|------|---------------|------------------|------------|
| | RADIUS | 1812 | XXXXXXXXXX | 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 | | | | | |
| | RADIUS | 1812 | XXXXXXXXXX | 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 | | | | | |
| | RADIUS | 1812 | XXXXXXXXXX | 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 | | | | | |
| | RADIUS | 1812 | XXXXXXXXXX | 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

665656

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 8-14](#) 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 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.

Local SA Bindings

Selecting the Local SA Bindings link takes you to the Local SA Bindings page (Figure 6-5). 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 6-5 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 86867

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 6-6).

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 6-6 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 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. If multiple authoritative access points are configured, their IP addresses are displayed.

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. In addition, the home agent also issues gratuitous ARPs for the mobile node in case there are nodes who could not hear the mobile node.

View Subnet Map Table

Selecting the View Subnet Map Table link takes you to the Subnet Map Table page (Figure 6-7). 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 6-7:

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

Figure 6-7 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 | | | |

86861

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.

Before You Begin

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.

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 items:

- 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).

Configuring the Authoritative Access Point

Proxy Mobile IP must be enabled on the wireless SSID. Since multiple SSIDs may exist on the access point and not all SSIDs may have to accommodate mobile clients, you must enable proxy Mobile IP per SSID. The AAP is used to communicate with new access points to update subnet map records and send the new access points a new and complete subnet mapping table. The AAP also contacts all the other access points listed in the table and sends update packets containing the changed information. In this way the other access points update their subnet mapping tables. For example, if a mobile device appears with a “30” subnet IP address on the “20” subnet, the access point must register the client with the home agent that services the mobile clients on the “30” subnet.

Follow these steps to configure the authoritative access point.

-
- 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.
 - Step 3** Select the SSID you intend to use by mobile clients and click **Edit**. The AP Radio: Internal SSID #x page appears ([Figure 6-8](#)).

Figure 6-8 AP Radio Internal SSID #x Page

Uptime: 4 days, 01:38:36

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-

| | Open | Shared | Network-EAP |
|---------------------------------|-------------------------------------|--------------------------|--------------------------|
| Accept Authentication Type: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Require EAP: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Default Unicast Address Filter: | Allowed | Allowed | Allowed |

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

Apply OK Cancel Restore Defaults

83998

Step 4 Set the Proxy Mobile IP setting to **yes**.

Step 5 Click **OK**. You are returned to the AP Radio: Internal Service Sets page.

Step 6 Click **OK** again. You are returned to the Setup page.

Step 7 In the Services section, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears (Figure 6-9).

Figure 6-9 Proxy Mobile IP Setup Page

Uptime: 00:19:57

Home Map Network Associations Setup Logs Help

General

Authentication Server

Local SA Bindings

Statistics

View Subnet Map Table

Done

83998

Step 8 Click **General**. The Proxy Mobile IP General page appears (Figure 6-10).

Figure 6-10 Proxy Mobile IP General Page

- Step 9** Set the Enable Proxy Mobile IP setting to **yes**.
- Step 10** Enter the IP address of the access point in the Authoritative AP 1 field.
- Step 11** Click **OK**. You are returned to the Proxy Mobile IP Setup page.
- Step 12** Click **View Subnet Map Table**. The Subnet Map Table appears (Figure 6-11).

Figure 6-11 Subnet Map Table

| HA Address | Subnet Mask |
|------------|---------------|
| 10.30.0.1 | 255.255.255.0 |
| 10.20.0.1 | 255.255.255.0 |

- Step 13** Check the IP addresses in the HA Address column. The home agent's IP address should appear in this column.

Configuring the Access Point on a Home or Foreign Network

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 and be detected by the authoritative access point.

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 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.

Follow these steps to configure a home or foreign agent access point.

-
- Step 1** Configure the access point normally (SSID, security, etc.).
 - Step 2** From the Associations section of the Setup page, select the SSID for the radio you are configuring. The Service Set Summary Status page appears.
 - Step 3** Highlight the SSID you are using for the mobile nodes and click **Edit**. The AP Radio Internal SSID #*n* appears.
 - Step 4** Set the Proxy Mobile IP is enabled radio button to **yes** and click **OK** to return to the Service Set Summary Status page.
 - Step 5** Click **OK** again to return to the Setup page.
 - Step 6** In the Services section of the Setup page, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears.
 - Step 7** Click **General**. The Proxy Mobile IP General page appears.
 - Step 8** Set the Enable Proxy Mobile IP radio button to **yes**.
 - Step 9** Enter the IP address of the authoritative access point in the Authoritative AP 1: field.
 - Step 10** Click **OK** to return to the Proxy Mobile IP Setup page.
 - Step 11** Click **Local SA Bindings**. The Local SA Bindings page appears.
 - Step 12** Enter the starting and ending IP addresses of the range of IP addresses designated as valid mobile node addresses.
 - Step 13** Enter a predetermined SPI and Group Key in the appropriate fields.
 - Step 14** Click **OK** to return to the Proxy Mobile IP Setup page.
 - Step 15** Click **Done** to return to the Setup page.
-