



Mobile Access Router and Mesh Networks Design Guide

The Cisco 3200 Series Mobile Access router (also referred to as the MAR3200 or the mobile access router (MAR)) is a compact, high-performance access solution that offers seamless mobility and interoperability across wireless networks. This guide describes how to use the MAR3200 in mesh networks for communicating mission-critical voice, video, and data.

Contents

Introduction	2
MAR3200 Interfaces	2
MAR3200 WMIC Features	5
Universal Workgroup Bridge Considerations	6
MAR3200 Management Options	7
Using the MAR with a Cisco 1500 Mesh AP Network	7
Vehicle Network Example	8
Simple Universal Bridge Client Data Path	8
Configuration Examples	10
Connect to the Cisco 3200 Series Router	10
Configure the IP Address, DHCP, and VLAN on the MAR	10
WMIC Configurations	11
WMIC Universal Bridge Client Configuration	11
WMIC Bridge Configuration	11
Configuring the WMIC to Serve as an Access Point	12
Security	13
Authentication Types	13
Open Authentication to the WMIC	13

Shared Key Authentication to the WMIC	14
EAP Authentication to the Network	14
MAC Address Authentication to the Network	16
Key Management	17
Using CCKM Key Management	17
Using WPA Key Management	17
Security Configuration	17
Assigning Authentication Types to an SSID	18
Configuring Authentication Types for 2.4 WMIC Radios	19
EAP-TLS Authentication with AES Encryption Example	21
Configuring the Root Device Interaction with WDS	22
Configuring Additional WPA Settings	22
WPA and Pre-Shared Key Configuration Example	23
Matching Authentication Types on Root and Non-Root Bridges	23
Using the MAR3200 in Mobile Environments	24
WMIC Roaming Algorithm	24
Using Network Address Translation (NAT) with the MAR3200	25
MAR3200 in Mobile IP Environments	26
The MAR 3200 Mobile IP Registration Process	26
Mobile IP Configuration	28
Basic HA and Foreign Agent Router Configurations	28
Configuring OSPF Routing Between HA, FA1, and FA2	28
Configuring IP Address, DHCP, and VLAN on the MR	29
Configuring a 2.4GHz Access Point on the MR	29
Configuring the 2.4 Universal Work Group Bridge Client	30
Configuring the Home Agent (HA)	31
Configuring the Foreign Agent (FA)	32
Configuring the Mobile Router (MR)	33
Verifying the Mobile IP Configuration	33

Introduction

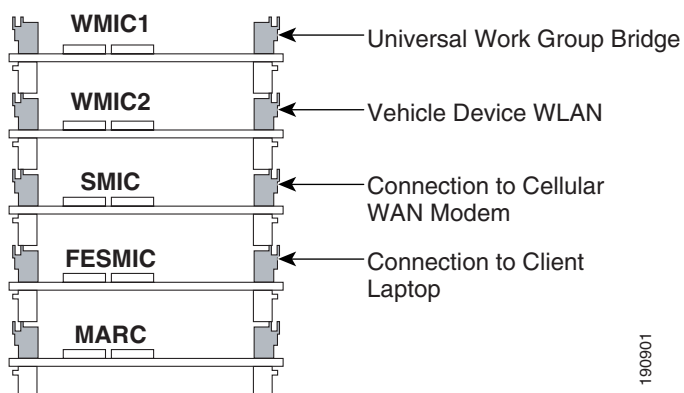
The size of the Cisco MAR3200 (see [Figure 1](#)) makes it ideal for use in vehicles in public safety, homeland security, and transportation sectors. The MAR3200 delivers seamless mobility across multiple radio, cellular, satellite, and wireless LAN (WLAN) networks, and can communicate mission-critical voice, video, and data across peer-to-peer, hierarchical, or meshed networks.

Figure 1 Cisco 3200 Series Mobile Access Router



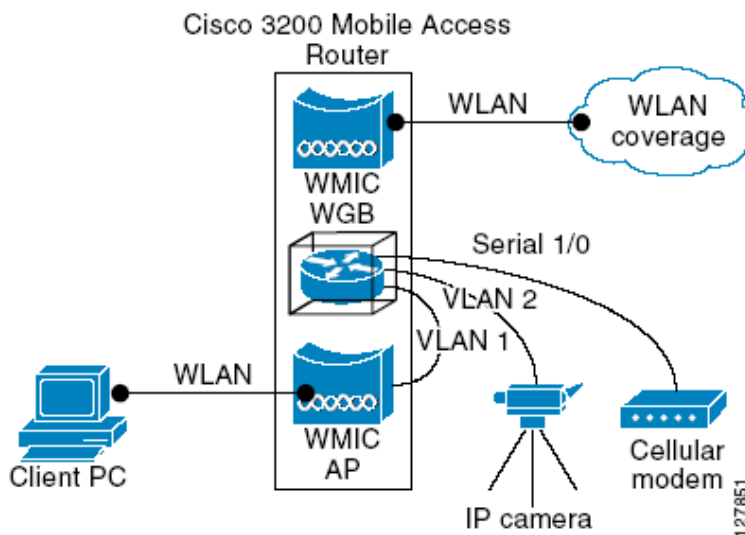
MAR3200 Interfaces

The MAR3200 can be configured with multiple Ethernet and serial interfaces, and up to three radios. The router itself is made up of stackable modules referred to as *cards*. [Figure 2](#) shows the stackable card configuration. The MAR3200 has two 2.4GHz Wireless Mobile Interface Cards (WMICs) one 4.9GHz WMIC, one Fast Ethernet Switch Mobile Interface Card (FESMIC) and one Mobile Access Router Card (MARC)). The MR can also be configured in a rugged enclosure with power adapters.

Figure 2 Card Connections

For more information on MAR3200 configuration options, refer to the following URL:
http://www.cisco.com/en/US/prod/collateral/routers/ps272/product_data_sheet0900aecd800fe973.html

Figure 3 provides an example of a MAR3200 configured with two WMICs, an FESMIC, and a MARC.

Figure 3 Mobile Unit Configuration Example

The following tables list the port-to-interface relationships and hardware types. Refer to these tables for configurations where you need to plug other devices into the MAR3200.

Table 1 shows the setup of WMICs on the Cisco 3230 Mobile Access router.

Table 1 WMIC Ports

	Internal Wiring Ports	Radio Type
WMIC 1 (W1)	FastEthernet 0/0	2.4GHz
WMIC 2 (W2)	FastEthernet 2/3	2.4GHz
WMIC 3 (W3)	FastEthernet 2/2	4.9GHz

Table 2 shows the setup of serial interfaces on the Cisco 3230 Mobile Access router.

Table 2 SMIC Ports

	Internal Wiring Ports	Interface Type
Serial 0	Serial 1/0	DSCC4 Serial
Serial 1	Serial 1/1	DSCC4 Serial
Internal	Serial 1/2	DSCC4 Serial
Internal	Serial 1/3	DSCC4 Serial

Table 3 shows the setup of Fast Ethernet interfaces on the Cisco 3230 Mobile Access router.

Table 3 *Fast Ethernet Ports*

	Internal Wiring Ports	Interface Type
Internal WMIC 1	Fast Ethernet 0/0	Fast Ethernet
FE0X	Fast Ethernet 2/0	Fast Ethernet
FE1X	Fast Ethernet 2/1	Fast Ethernet
Internal WMIC 3	Fast Ethernet 2/2	Fast Ethernet
Internal WMIC 2	Fast Ethernet 2/3	Fast Ethernet

MAR3200 WMIC Features

Table 4 highlights the software features of WMICs running Cisco IOS.

Table 4 *WMIC IOS Software Features*

Feature	Description
VLANs	Allows dot1Q VLAN trunking on both wireless and Ethernet interfaces. Up to 32 VLANs can be supported per system.
QoS	Use this feature to support quality of service for prioritizing traffic on the wireless interface. The WMIC supports required elements of Wi-Fi Multimedia (WMM) for QoS, which improves the user experience for audio, video, and voice applications over a Wi-Fi wireless connection and is a subset of the IEEE 802.11e QoS specification. WMM supports QoS prioritized media access through the Enhanced Distributed Channel Access (EDCA) method.
Multiple BSSIDs	Supports up to 8 BSSIDs in access point mode.
RADIUS accounting	When running the WMIC in access point (AP) mode you can enable accounting on the WMIC to send accounting data about authenticated wireless client devices to a RADIUS server on your network.
TACACS+ administrator authentication	TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. It provides secure, centralized validation of administrators attempting to gain access to your WMIC.
Enhanced security	Supports three advanced security features: <ul style="list-style-type: none"> • WEP keys: Message Integrity Check (MIC) and WEP key hashing CKIP • WPA • WPA2
Enhanced authentication services	Allows non-root bridges or workgroup bridges to authenticate to the network like other wireless client devices. After a network username and password for the non-root bridge or workgroup bridge are set, (LEAP), EAP-TLS or EAP-FAST can be used for authentication in dynamic WEP, WPA, or WPA2 configurations.
802.1x supplicant	In AP mode, the Mobile Access Router supports standard 802.1x EAP types for WLAN clients.

Table 4 WMIC IOS Software Features (continued)

Fast secure roaming	Fast, secure roaming using Cisco Centralized Key Management (CCKM) in Work Group Bridge mode and Universal Work Group Bridge mode.
Universal workgroup bridge	Supports interoperability with non-Cisco APs.
Repeater mode	Allows the access point to act as a wireless repeater to extend the coverage area of the wireless network.

Universal Workgroup Bridge Considerations

The Cisco Compatible eXtensions (CCX) program delivers advanced WLAN system level capabilities and Cisco-specific WLAN innovations to third party Wi-Fi-enabled laptops, WLAN adapter cards, PDAs, WI-FI phones, and application specific devices (ASDs). The 2.4 GHz WMIC provides CCX client support. When the 2.4 GHz WMIC is configured as a universal workgroup bridge client, it does not identify itself as a CCX client. However, it does support CCX features. [Table 5](#) lists the supported features.

Table 5 CCX Version Feature Support

Feature	v1	v2	v3	v4	AP	WGB	WGB Client
Security							
Wi-Fi Protected Access (WPA)		X	X	X	X	X	X
IEEE 802.11i - WPA2			X	X	X	X	X
WEP	X	X	X	X	X	X	X
IEEE 802.1X	X	X	X	X	X	X	X
LEAP	X	X	X	X	X	X	X
EAP-FAST			X	X	X	X	X
CKIP (encryption)	X				X	X	
Wi-Fi Protected Access (WPA): 802.1X + WPA TKIP		X	X	X	X	X	X
With LEAP		X	X	X	X	X	X
With EAP-FAST			X	X	X	X	X
IEEE 802.11i- WPA2: 802.1X+AE			X	X	X	X	X
With LEAP			X	X	X	X	X
With EAP-FAST			X	X	X	X	X
CCKM EAP-TLS				X	X	X	X
EAP-FAST				X	X	X	X
Mobility							
AP-assisted roaming		X	X	X	X	X	X
Fast re-authentication via CCKM, with LEAP		X	X	X	X	X	X

Table 5 CCX Version Feature Support (continued)

Fast re-authentication via CCKM with EAP-FAST			X	X	X	X	X
MBSSID				X	X		
Keep-Alive				X	X	X	
QoS and VLANs							
Interoperability with APs that support multiple SSIDs and VLANs	X	X	X	X	X	X	
Wi-Fi Multimedia (WMM)			X	X	X	X	X
Performance and Management							
AP-specified maximum transmit power		X	X	X	X	X	X
Recognition of proxy ARP information element (For ASP)			X	X	X		
Client Utility Standardization							
Link test				X	X	X	X

MAR3200 Management Options

You can use the WMIC management system through the following interfaces:

- The IOS command-line interface (CLI), which you use through a PC running terminal emulation software or a Telnet/SSH session.
- Simple Network Management Protocol (SNMP).
- Web GUI management.

Using the MAR with a Cisco 1500 Mesh AP Network

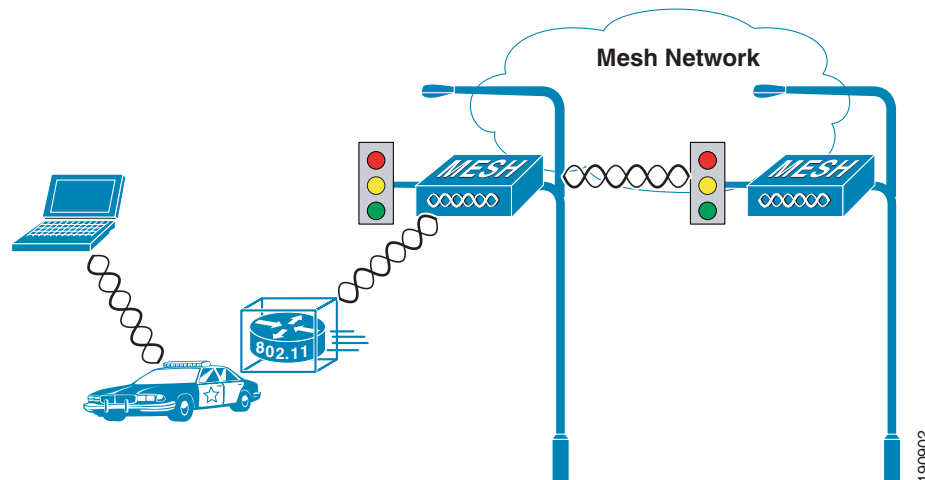
The Universal Workgroup Bridge feature for the Cisco MAR3200 WMIC allows the WMIC radio to associate to non-Aironet based access points. It also supports a majority of CCXv4 client features. In the version 4.0 software release for the Cisco Wireless LAN Controller (WLC), and Mesh APs, enhancements have been added to support Cisco 1230, 1240, 1130, or 3200 products associating to the Cisco 1500 as a workgroup bridge (WGB). These two feature updates allow the MAR to act as a client to the 1500 Mesh AP networks or Light Weight Access Point Protocol (LWAPP) WLAN networks enabling new solutions for public safety, commercial transportation, and defense markets. The MAR not only has Fast Ethernet and Serial interface connections for other client devices, but can also use them to connect to other network devices for backhaul purposes.

Vehicle Network Example

This section describes a simple application for the MAR3200 in a Mesh network using its universal workgroup bridge feature to connect to the Mesh WLAN. Figure 4 illustrates this example.

- A Cisco 3200 Series router installed in a mobile unit allows the client devices in and around the vehicle to stay connected while the vehicle is roaming.
- WMICs in vehicle-mounted Cisco 3200 Series routers are configured as access points to provide connectivity for 802.11b/g and 4.9-GHz wireless clients.
- Ethernet interfaces are used to connect any in-vehicle wired clients, such as a laptop, camera, or telematics devices, to the network.
- Another WMIC is configured as a Universal Workgroup Bridge for connectivity to a Mesh AP, allowing transparent association and authentication through a root device in the architecture as the vehicle moves about.
- Serial interfaces provide connectivity to wireless WAN modems that connect to cellular networks such as CDMA or GPRS. The Wireless 802.11 connections are treated as preferred services because they offer the most bandwidth. However, when a WLAN connection is not available, cellular technology provides a backup link. Connection priority can be set by routing priority, or by the priority for Mobile IP.

Figure 4 Vehicle Network Example



Simple Universal Bridge Client Data Path

The IP devices connected to the MAR are not *aware* that they are part of a mobile network. When they must communicate with another node in the network, their traffic is sent to their default gateway, the Cisco 3200 Series router. The Cisco 3200 Series router forwards the traffic to the Mesh APs WLAN, the mesh AP then encapsulates the data packets in LWAPP and forwards them through the network to the controller.

As shown in Figure 5, the Cisco 3200 Series router sends traffic over the Universal Bridge Client WLAN backhaul link. This traffic then crosses the WLAN to the controller where it is then forwarded out the controller interface to the wired network. Return traffic destined for any client attached to the MAR

would be forwarded via a static route pointing back to the controller of the Mesh network. Figure 6 shows the return path to the MAR. Mobile IP eliminates the need for static routing and is covered later in this document. NAT can be used in simple deployments when Mobile IP is not available.

The data path example shown in Figure 5, and previously described, represents the traffic in a pure Layer 2 Mesh when the MAR is using only the WMIC for backhaul. If the deployment calls for more complexity (such as secondary cellular backhaul links) then Mobile IP is required.

When the WMIC is used as a Universal Bridge Client, it sets up its wireless connections the same way any wireless client does.

Figure 5 Simple Layer 2 Data Path Example

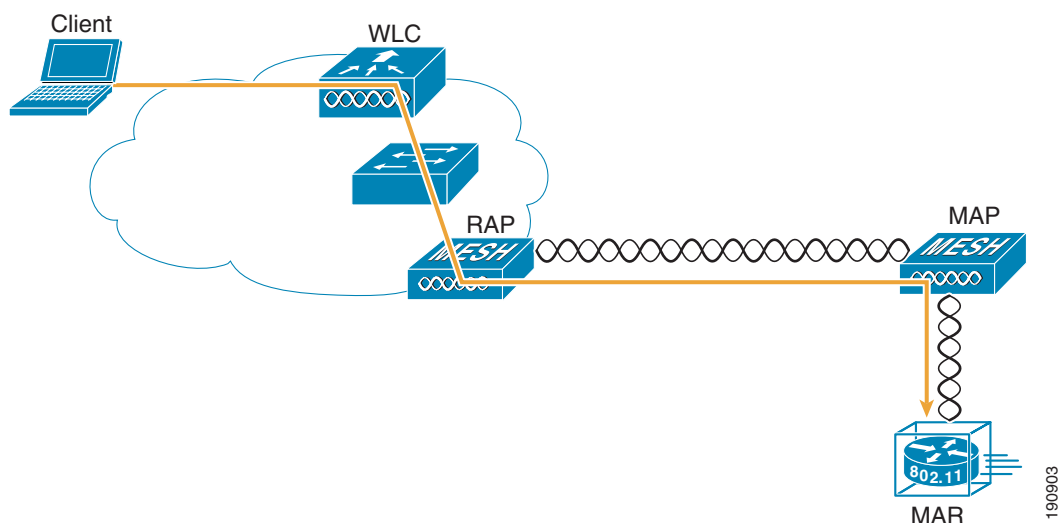
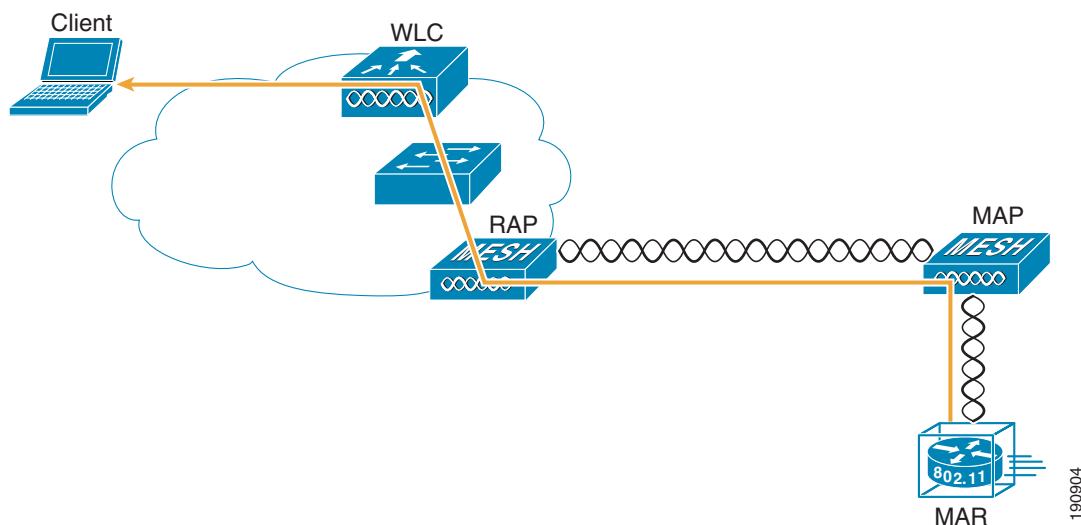


Figure 6 Client Return Data Path



Configuration Examples

This section provides configuration examples for the Cisco 3200 Series router.

Connect to the Cisco 3200 Series Router

Attach the console cable to both the serial port of your PC and the Mobile Access router console port (DB9 socket). Use a straight-through DB9-to-DB9 cable.

Configure the IP Address, DHCP, and VLAN on the MAR

- Step 1** Connect to and log in to the MAR. Create a loopback interface and assign an IP address:

```
bridge(config)# int loopback 0
bridge(config-if)# ip address 24.24.24.24 255.255.255.255
```

- Step 2** To create VLAN 2 in the VLAN database, enter:

```
bridge# vlan database
```

- Step 3** Configure the VLAN 3 and VLAN 2 interfaces. VLAN 3 is used for the 2.4 GHz WMIC2 (W2) which is acting as AP and VLAN 2 is used for the 4.9GHz WMIC (W3). Configure FA2/0, FA2/1 and FA2/3 to be in VLAN 3, and FA 2/2 to be in VLAN 2.

- Step 4** Create VLAN 4 in the VLAN database for connection between WMIC 1 and the MARC.

Connected to	Interface	Radio Type	VLAN	Description
PC	FastEthernet2/0	None	3	Fast Ethernet link for end device
WMIC 1 (W1)	FastEthernet0/0	2.4GHz	4	2.4 GHz Universal Work Group Bridge connection to Mesh Network
WMIC 2 (W2)	FastEthernet2/3	2.4GHz	3	Provide 2.4 GHz AP Hotspot around the mobile router
WMIC 3 (W3)	FastEthernet2/2	4.9GHz	2	4.9GHz uplink as Workgroup Bridge

- Step 5** Configure the DHCP server for VLAN 3 using following commands:

```
bridge(config)# ip dhcp pool mypool
bridge(dhcp-config)# network 10.40.10.0 /28
bridge(dhcp-config)# default-router 10.40.10.1
bridge(config)# ip dhcp excluded-address 10.40.10.1 10.40.10.3
```

- Step 6** Verify that the wired client on VLAN 3 has been assigned a DHCP IP address in the 10.40.10.0/28 subnet.

WMIC Configurations

This section provides information on the various WMIC configurations.

WMIC Universal Bridge Client Configuration

The WMIC can be configured as a universal workgroup bridge. In this role, the WMIC has the following functionality:

- Associates to the IOS and non-IOS access points.
- Interoperability—A universal workgroup bridge can forward routing traffic using a non-Cisco root device as a universal client. The universal workgroup bridge appears as a normal wireless client to the root device. As a root device, the WMIC supports Cisco-compatible extension clients, with all CCXv3 features and many CCXv4 features.

To configure the WMIC as a Universal Workgroup Bridge, enter the following command:

```
bridge(config)# station-role workgroup-bridge universal [mac address]
```



Note

You must use the mac-address of the associated VLAN that the WMIC is bridged to. As an example, we will use the mac-address of VLAN 1. To acquire the MAC address of VLAN 1, console in to the MARS router card and enter the **show mac-address-table** command.

WMIC Bridge Configuration

The WMIC can be configured as a bridge. There are three install modes: automatic, root, and non-root:

- Automatic mode activates the bridge install and alignment mode, and specifies that the device automatically determines the network role. If the device is able to associate to another Cisco root device within 60 seconds, it assumes a non-root bridge role; otherwise it assumes a root device role. The device can be configured into root device or non-root bridge modes to avoid the 60-second automatic detection phase.
- Root mode specifies that the device is operating as a root device and connects directly to the main Ethernet LAN network. In this mode, the unit accepts associations from other Cisco bridges and wireless client devices.
- Non-root mode specifies that the device is operating as a non-root bridge, and that it connects to a remote LAN network, and that it must associate with a Cisco root device by using the wireless interface. Bridge mode is the only mode that supports the **distance** command.

The **distance** command specifies the distance from a root device to its clients (non-root bridges and/or workgroup bridges). The distance setting adjusts the time out values to account for the time required for radio signals for radio signals to travel from a root device to its clients (non-root bridges and/or workgroup bridges). In installation mode, the default distance setting a 2.4-GHz WMIC is 99 km for maximum delay spread during antenna alignment. In other modes, the default distance setting is 0 km. Changing to a different mode sets the distance to the default distance. If more than one non-root bridge (or workgroup bridge) communicates with the root device, enter the distance from the root device to the non-root bridge (or work-group bridge) that is farthest away. Enter a value from 0 to 99 km for a 2.4-GHz WMIC or 0 to 3 km for a 4.9-GHz WMIC. You do not need to adjust this setting on non-root bridges.

To configure the WMIC to determine its role automatically, perform the following steps:

Step 1 To enter global configuration mode, enter:

```
bridge# configure terminal
```

Step 2 To enter configuration mode for the radio interface, enter:

```
bridge(config)# interface dot11radio port
```

Step 3 To configure the WMIC's bridge role, enter the following commands:

```
bridge(config-if)# station-role {root [bridge |  
bridge(config-if)# non-root workgroup-bridge install [automatic | root | non-root]}
```

The **station-role** command specifies that role of the WMIC is chosen based on the device to which it is associated.

Set the WMIC role:

- To specify that MAR3200 WMIC operates as the root bridge device, use the **station-role root bridge** command. This mode does not support wireless client associations.
- To specify that the MAR3200 WMIC operates in workgroup bridge mode, use the **station-role workgroup-bridge** command. As a workgroup bridge, the device associates to an Aironet access point or bridge as a client and provides a wireless LAN connection for devices connected to its Ethernet port.

Step 4 Enter a distance setting from 0 to 99 km for a 2.4-GHz WMIC or 0 to 3 km for a 4.9-GHz WMIC:

```
bridge(config-if)# distance kilometers
```

Step 5 Use the **mobile station** command to configure a non-root bridge or workgroup bridge as a mobile station. When this feature is enabled, the bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, the WMIC searches for a new root association and roams to a new root device before it loses its current association. When the mobile station setting is disabled (the default setting) the WMIC does not search for a new association until it loses its current association.

Step 6 Enter the **end** command to complete the configuration.

Step 7 To make a backup copy of the configuration, enter:

```
bridge# copy running-config startup-config
```

Configuring the WMIC to Serve as an Access Point

The WMIC can be configured as a root access point. In this role, it accepts associations from wireless clients. This can be a useful configuration if you are planning to deploy a mobile hotspot.

To configure the WMIC as an access point, perform the following steps:

Step 1 To enter global configuration mode, enter:

```
bridge# configure terminal
```

Step 2 To specify the interface configuration mode for the radio interface, enter:

```
bridge(config)# interface dot11radio port
```

- Step 3** To specify the SSID the AP will use, enter:
- ```
bridge(config-if)# ssid given ssid
```
- Step 4** To specify the authentication type to be used, enter:
- ```
bridge(config-if)# authentication open
```
- Step 5** To specify the radio channel the AP will operate on, enter:
- ```
bridge(config-if)# channel 11
```
- Step 6** To specify for the WMIC to function as a root access point, enter:
- ```
bridge(config-if)# station-role root access-point
```
- Step 7** Enter the **end** command to complete the configuration.
- Step 8** To make a backup copy of the configuration, enter:
- ```
bridge# copy running-config startup-config
```
- 

## Security

This section describes the security features of the WMIC.

### Authentication Types

This section describes the authentication types that you can configure on the WMIC. The authentication types are tied to the SSID that you configure on the WMIC. Before wireless devices can communicate, they must authenticate to each other using open, 802.1x/EAP based or shared-key authentication. For maximum security, wireless devices should also authenticate to your network using EAP authentication, an authentication type that relies on the presence of an authentication server on your network.

The WMIC uses four authentication mechanisms or types and can use more than one at the same time.

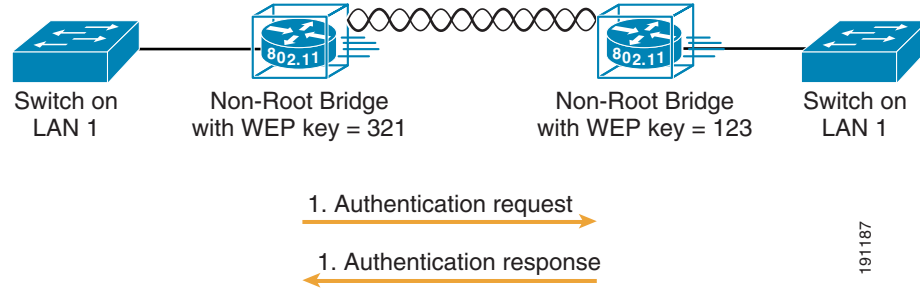
These sections explain each authentication type:

- [Open Authentication to the WMIC, page 14](#)
- [Shared Key Authentication to the WMIC, page 15](#)
- [EAP Authentication to the Network, page 15](#)
- [MAC Address Authentication to the Network, page 17](#)

### Open Authentication to the WMIC

Open authentication allows any wireless device to authenticate and then attempt to communicate with another wireless device. Open authentication does not rely on a RADIUS server on your network.

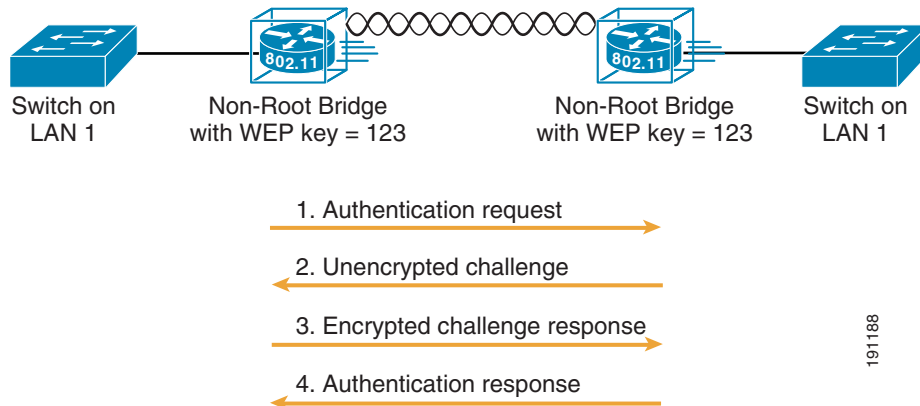
[Figure 7](#) shows the authentication sequence between a non-root bridge and a root device using open authentication. In this example, the non-root bridge's WEP key does not match the bridge's key, so it can authenticate but it cannot pass data.

**Figure 7 Open Authentication**

## Shared Key Authentication to the WMIC

Cisco provides shared key authentication to comply with the IEEE 802.11b and IEEE 802.11g standards. However, because of shared key's security flaws, we recommend that you use another method of authentication, such as EAP, in environments where security is an issue. During shared key authentication, the root device sends an unencrypted challenge text string to the client device that is attempting to communicate with the root device. The client device requesting authentication encrypts the challenge text and sends it back to the root device.

Both the unencrypted challenge and the encrypted challenge can be monitored, which leaves the root device open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Figure 8 shows the authentication sequence between a device trying to authenticate and a bridge using shared key authentication. In this example the device's WEP key matches the bridge's key, so it can authenticate and communicate.

**Figure 8 Sequence for Shared Key Authentication**

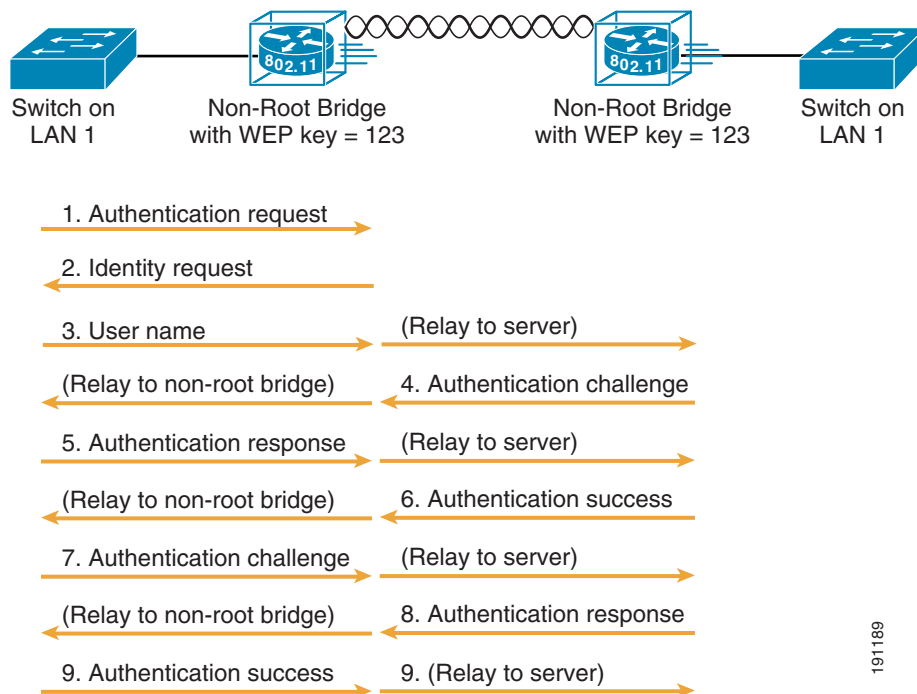
## EAP Authentication to the Network

This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the root device helps the authenticating device and the RADIUS server perform mutual authentication and derive a dynamic session key, which is used by both the root and authenticating devices to further derive the unicast key. The root generates the broadcast key and sends it to the authenticating device after

encrypting it with a unicast key. The unicast key is used to exchange unicast data between the root device and authenticated device, and the broadcast key is used to exchange multicast and broadcast data between them.

When you enable EAP on your bridges, authentication to the network occurs in the sequence shown in Figure 9.

**Figure 9 EAP Authentication**



In Steps 1 through 9 in Figure 9, a non-root bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root device:

- The RADIUS server sends an authentication challenge to the non-root bridge.
- The non-root bridge uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server.
- Using information from its user database, the RADIUS server creates its own response and compares that to the response from the non-root bridge.
- When the RADIUS server authenticates the non-root bridge, the process repeats in reverse, and the non-root bridge authenticates the RADIUS server.
- When mutual authentication is complete, the RADIUS server and the non-root bridge determine a session key that is unique to this session between the RADIUS server and non-root bridge and provide the non-root bridge with the appropriate level of network access.
- The RADIUS server encrypts and transmits the session key over the wired LAN to the root device.
- The root device and the non-root bridge derive the unicast key from the session key. The root device generates the broadcast key and sends it to the non-root bridge after encrypting it with the unicast key.



- The non-root bridge uses the unicast key to decrypt the broadcast key. The non-root bridge and the root device activate WEP and use the unicast and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the bridge behaves the same way for each type. It relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device.

(If you use EAP authentication, you can optionally select open or shared key authentication, as well as EAP authentication controls authentication both to your bridge and to your network.)

## EAP-TLS

EAP-TLS uses public key infrastructure (PKI) to acquire and validate digital certificates. A digital certificate is a cryptographically signed structure that guarantees the association between at least one identifier and a public key. It is valid for a limited time period and use, subject to certificate policy conditions. The Certificate Authority (CA) issues certificates to client and server. The supplicant and the back-end RADIUS server must both support EAP-TLS authentication. The root device acts as an AAA Client and is also known as the network access server (NAS). The root devices must support 802.1x/EAP authentication process even though they are not aware of the EAP authentication protocol type. The NAS tunnels the authentication messages between the peer (user machine trying to authenticate) and the AAA server (such as the Cisco ACS). The NAS is aware of the EAP authentication process only when it starts and ends.

## EAP-FAST

EAP-FAST encrypts EAP transactions within a TLS tunnel. The TLS tunnel encryption helps prevent dictionary attacks that are possible using LEAP. The EAP-FAST tunnel is established using shared secret keys that are unique to users. Because handshakes that are based on shared secrets are intrinsically faster than handshakes that are based on a PKI infrastructure, EAP-FAST is significantly faster than PEAP and EAP-TLS.

EAP-FAST operates according to the following three phases:

- Delivery of a key to the client
- Establishment of a secure tunnel using the key
- Authentication of the client over the secure tunnel

After successful client authentication to the EAP-FAST server, a RADIUS access-accept message is passed to the root device (along with the master session key) and an EAP success message is generated at the root device (as with other EAP authentication protocols). Upon receipt of the EAP-success packet, the client derives a session key using an algorithm that is complimentary to the one used at the server to generate the session key passed to the root device.

## MAC Address Authentication to the Network

The access point relays the wireless client device's MAC address to a RADIUS server on the network, and the server checks the address against a list of allowed MAC addresses. Because intruders can create counterfeit MAC addresses, MAC-based authentication is less secure than EAP authentication.

However, MAC-based authentication does provide an alternate authentication method for client devices that do not have EAP capability or can be used as a addition to EAP.

## Key Management

This section describes the available key management features.

### Using CCKM Key Management

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one AP to another without any perceptible delay during reauthentication. An LWAPP AP on the network provides secure fast roaming, when the WLC creates a cache of security credentials for CCKM-enabled devices on the subnet. The WLC cache of credentials dramatically reduces the time required for reauthentication when a CCKM-enabled client device roams to an AP. When a client device roams and tries to reauthenticate to a new AP served by the same WLC or a WLC belonging to the same mobility group, the WLC authenticates the client using its cache of client's credentials rather than requiring RADIUS server to authenticate the client. The reassociation process is reduced to a two-packet exchange between the roaming client device and the new AP. Roaming client devices reauthentication quickly enough for there to be no perceptible delay in voice or other time-sensitive applications

### Using WPA Key Management

Wi-Fi Protected Access (WPA) is a standards-based interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. WPA is derived from the IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) for data protection.

WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-Shared key (WPA-PSK). Using WPA key management, the client device and the authentication server authenticate with each other using the EAP authentication method, and the client device and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the root device. With WPA-PSK, you configure a pre-shared key on both the client device and the root device, and that pre-shared key is used as the PMK.



#### Note

Unicast and multicast cipher suites advertised in the WPA information element (and negotiated during 802.11 association) could potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new VLAN ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the root device and the client device to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the non-root bridge is disassociated from the wireless LAN.)

## Security Configuration

The default configuration for the WMIC in AP mode has an SSID of autoinstall, which is also configured as guest mode. In guest mode, the WMIC broadcasts this SSID in its beacon and allows client devices with no SSID to associate.



#### Note

By default, the authentication type assigned to autoinstall is open. This enables clients with no security settings to connect to the MAR3200. In order to secure the MAR, this configuration default must be changed.

## Assigning Authentication Types to an SSID

From privileged EXEC mode, follow these steps to configure authentication types for SSIDs, such as an AP, root bridge, or non-root bridge, on the root device:

- Step 1** To enter global configuration mode for the router, enter:

```
bridge# configure terminal
```

- Step 2** To create an SSID, enter:

```
bridge(config)# dot11 ssid ssid-string
```

The SSID can consist of up to 32 alphanumeric characters. SSIDs are case-sensitive.

- Step 3** (Optional) To set the authentication type to “open” for this SSID, enter:

```
bridge(config-ssid)# authentication open [mac-address list-name [alternate]] [[optional] eap list-name]
```

Open authentication allows any client device to authenticate and then attempt to communicate with the WMIC.

- Step 4** (Optional) Set the SSID's authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Use the **alternate** keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network.

- Step 5** (Optional) Set the SSID's authentication type to open with EAP authentication. The WMIC forces all other client devices to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Use the **optional** keyword to allow client devices using either open or EAP authentication to associate and become authenticated. This setting is used mainly by service providers that require special client accessibility.



**Note** A root device configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot communicate with the root device.

For more information on method lists, refer to the following URL:

[http://www.cisco.com/en/US/docs/ios/12\\_2/security/configuration/guide/scfathen.html](http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfathen.html).

- Step 6** (Optional) Use the following command to set the authentication type for the SSID to “shared key:”

```
bridge(config-ssid)# authentication shared [mac-address list-name] [eap list-name]
```



**Note** Because of security flaws associated with using shared key, we recommend that you avoid using it. You can assign shared key authentication to only one SSID.

- Step 7** (Optional) Set the SSID's authentication type to shared key with MAC address authentication. For *list-name*, specify the authentication method list.

- Step 8** (Optional) Set the SSID's authentication type to shared key with EAP authentication. For *list-name*, specify the authentication method list.

- Step 9** (Optional) Set the authentication type for the SSID to use EAP for authentication and key distribution by entering:

```
bridge(config-ssid)# authentication network-eap list-name [mac-address list-name]
```

**Step 10** (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For list-name, specify the authentication method list.

**Step 11** (Optional) Set the key-management type for the SSID to WPA, CCKM, or both:

```
bridge(config-ssid)# authentication key-management {[wpa] [cckm]} [optional]
```

If you use the **optional** keyword, client devices not configured for WPA or CCKM can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.



**Note** Simultaneous use of WPA and CCKM is not supported with 802.11a radios.

Before you can enable CCKM or WPA, you must set the encryption mode to a cipher suite that includes TKIP/AES-CCMP. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP.

If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK.

To support CCKM, your root device must interact with the WDS device on your network.

**Step 12** To return to privileged EXEC mode, enter:

```
bridge(config-ssid)# exit
```

**Step 13** (Optional) To save your entries in the configuration file, enter:

```
bridge# copy running-config startup-config
```

## Configuring Authentication Types for 2.4 WMIC Radios

To configure authentication types for SSIDs on the non-root side, in privileged EXEC mode, perform the following steps:

**Step 1** To enter global configuration mode, enter:

```
bridge# configure terminal
```

**Step 2** To create the EAP profile, enter:

```
bridge(config)# eap profile profile-name-string
```

**Step 3** To create a dot1x credentials profile and enter the dot1x credentials configuration submode, enter:

```
bridge(config)# dot1x credentials profile
```

**Step 4** To choose an EAP authentication method for authentication purposes, enter:

```
bridge(config-eap-profile)# method [fast|gtc|leap|md5|mschapv2|tls]
```

**Step 5** Use the **exit** command to return to privileged EXEC mode.



**Note**

A device configured for EAP authentication forces all root devices that associate to perform EAP authentication. Root devices that do not use EAP cannot communicate with the device.

**Step 6** To enter global ssid mode, enter:

```
bridge(config)# dot11 ssid ssid-string
```

**Step 7** (Optional) To set the authentication type for the SSID to “use EAP for authentication and key distribution,” enter:

```
bridge(config-ssid)# authentication network-eap list-name
```

**Step 8** To create a dot1x credentials profile and enter the dot1x credentials configuration submode, enter:

```
bridge(config)# dot1x credentials profile
```

**Step 9** To specify the EAP profile, enter:

```
bridge(config-ssid)# dot1x eap profile profile-name-string
```

This is the profile you created in Step 2.

**Step 10** (Optional) To set the key-management type for the SSID to WPA, CCKM, or both, enter:

```
bridge(config-ssid)# authentication key-management {[wpa] [cckm]} [optional]
```

If you use the **optional** keyword, client devices that are not configured for WPA or CCKM can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable open authentication, network-EAP, or both.



**Note**

Only 802.11b and 802.11g radios support WPA and CCKM simultaneously.

Before you can enable CCKM or WPA, you must set the encryption mode to a cipher suite that includes TKIP/AES-CCMP. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP.

If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK.

**Step 11** Enter the **exit** command and then, optionally, enter the **copy running-config startup-config** command to create a copy of your configuration file.

## EAP-TLS Authentication with AES Encryption Example

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features. The following example sets the authentication type for the SSID *bridgeman* to open with EAP authentication. Bridges using the SSID *bridgeman* attempt EAP authentication using the eap method name *adam*. This example sets the authentication type for the SSID *bridgeman* to perform EAP-TLS authentication with AES encryption. Bridges using this SSID attempt EAP authentication using a server ID named *adam*.

```
bridge# configure terminal
bridge(config)# dot11 ssid bridgeman
bridge(config-ssid)# authentication open eap eap_adam
bridge(config-ssid)# authentication network-eap eap_adam
bridge(config-ssid)# authentication key-management wpa
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# exit
bridge(config)# interface dot11radio 0
bridge(config-if)# encryption mode ciphers aes-ccm
bridge(config-if)# ssid bridgeman
bridge(config-if)# end
```

The configuration on workgroup bridges, non-root bridges, and repeater bridges associated to this bridge would also contain these commands:

```
bridge# configure terminal
bridge(config)# eap profile authProfile
bridge(config-eap-profile)# method tls
bridge(config-eap-profile)# exit
bridge(config)# dot1x credentials authCredentials
bridge(config-dot1x-creden)# username adam
bridge(config-dot1x-creden)# password adam
bridge(config-dot1x-creden)# exit
bridge(config)# dot11 ssid bridgeman
bridge(config-ssid)# authentication open eap eap_adam
bridge(config-ssid)# authentication network-eap eap_adam
bridge(config-ssid)# authentication key-management wpa
bridge(config-ssid)# dot1x eap_profile authProfile
bridge(config-ssid)# dot1x credentials authCredentials
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# exit
bridge(config)# interface dot11radio 0
bridge(config-if)# encryption mode ciphers aes-ccm
bridge(config-if)# ssid bridgeman
bridge(config-if)# end
```

This example shows the RADIUS/AAA configuration on the root side for EAP authentication.

```
bridge# configure terminal
bridge(config)# aaa new-model
bridge(config)# aaa group server radius rad_eap
bridge(config-sg-radius)# server 13.1.1.99 auth-port 1645 acct-port 1646
bridge(config)# aaa authentication login eap_adam group rad_eap
bridge(config)# aaa session-id common
bridge(config)# radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7 141B1309
bridge(config)# radius-server authorization permit missing Service-Type
bridge(config)# ip radius source-interface BVI1
bridge(config)# end
```

## Configuring the Root Device Interaction with WDS

To support non-root bridges using CCKM, your root device must interact with the WDS device on your network, and your authentication server must be configured with a username and password for the root device. For more information on configuring WDS and CCKM on your wireless LAN, refer to Chapter 11 in the *Cisco IOS Software Configuration Guide for Cisco Access Points* at the following URL: [http://www.cisco.com/en/US/docs/wireless/access\\_point/12.4\\_10b\\_JA/configuration/guide/scg12410b-chap4-first.html](http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html).

---

**Step 1** On your root device, enter global configuration mode:

```
Router# configure terminal
```

**Step 2** Configure a username and password for the AP to use for authentication.

You must configure the same username and password pair when you set up the root device as a client on your authentication server:

```
bridge(configure)# wlccp ap username username password password
```

---

## Configuring Additional WPA Settings

This section provides information on the addition settings that can be configured for WPA.

### Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the bridge. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between eight and 63 characters, and the bridge expands the key using the process described in the Password-based Cryptography Standard (RFC2898). If you enter the key in hexadecimal characters, you must enter 64 hexadecimal characters.

### Configuring Group Key Updates

In the last step in the WPA process, the root device distributes a group key to the authenticated non-root bridge. You can use these optional settings to configure the root device to change and distribute the group key based on association and disassociation of non-root bridges:

- **Membership termination**—The root device generates and distributes a new group key when any authenticated non-root bridge disassociates from the root device. This feature keeps the group key private for associated bridges.
- **Capability change**—The root device generates and distributes a dynamic group key when the last non-key management (static WEP) non-root bridge disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) non-root bridge authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static WEP bridges associated to the root device.

To configure a WPA pre-shared key and group key update options, in privileged EXEC mode, perform the following steps:

**Step 1** To enter global configuration mode, enter:

```
bridge# configure terminal
```

**Step 2** To enter SSID configuration mode for the SSID, enter:

```
bridge(config)# dot11 ssid ssid-string
```

**Step 3** To specify a pre-shared key for bridges using WPA that also use static WEP keys, enter:

```
bridge(config)# wpa-psk { hex | ascii } [0 | 7] encryption-key
```

Enter this key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of eight letters, numbers, or symbols, and the bridge expands the key for you. You can enter a maximum of 63 ASCII characters.

**Step 4** Enter the **end** command to complete the configuration.

## WPA and Pre-Shared Key Configuration Example

This example shows how to configure a pre-shared key for non-root bridges using WPA and static WEP, with group key update options:

```
bridge# configure terminal
bridge(config)# dot11 ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(config-ssid)# end
```

## Matching Authentication Types on Root and Non-Root Bridges

To use the authentication types described in this section, the root device authentication settings must match the settings on the non-root bridges that associate to the root device.

[Table 6](#) lists the settings required for each authentication type on the root and non-root bridges.

**Table 6** *Client and Bridge Security Settings*

| Security Feature                          | Non-Root Bridge Setting                                    | Root Device Setting                                         |
|-------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------|
| Static WEP with open authentication       | Set up and enable WEP                                      | Set up and enable WEP and enable open authentication        |
| Static WEP with shared key authentication | Set up and enable WEP and enable shared key authentication | Set up and enable WEP and enable shared key authentication  |
| LEAP authentication                       | Configure a LEAP username and password                     | Set up and enable WEP and enable network-EAP authentication |



**Table 6**     *Client and Bridge Security Settings (continued)*

|                     |                                                      |                                                                                                                                                                                            |
|---------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CCKM key management | Set up and enable WEP and enable CCKM authentication | Set up and enable WEP and enable CCKM authentication, configure the root device to interact with your WDS device, and add the root device to your authentication server as a client device |
| WPA key management  | Set up and enable WEP and enable WPA authentication  | Set up and enable WEP and enable WPA authentication                                                                                                                                        |

## Using the MAR3200 in Mobile Environments

This section describes how the MAR is used in mobile environments.

### WMIC Roaming Algorithm

There are four conditions that will trigger the WMIC to start scanning for a better root bridge or access point:

- The loss of eight consecutive beacons
- A shift in the data rate
- The maximum data retry count is exceeded (the default value is 64 on the WMIC)
- A measured period of time of a drop in the signal strength threshold

Only the last two items in this list are configurable using the **packet retries** command and **mobile station period X threshold Y** (in dBm); the remainder are hard-coded. These commands are issued under the dot11 interface.

If a client starts scanning because of a loss of eight consecutive beacons, the message “Too many missed beacons” is displayed on the console. In this case, the WMIC is acting as a Universal Bridge Client, much like any other wireless client in its behavior.

An additional triggering mechanism, mobile station (if mobile station is configured), is not periodic but does have two variables: *period* and *threshold*.

The mobile station algorithm evaluates two variables: data rate shift and signal strength and responds as follows:

- If the driver does a long term down shift in the transmit rate for packets to the parent, the WMIC initiates a scan for a new parent (no more than once every configured period).
- If the signal strength (threshold) drops below a configurable level, the WMIC scans for a new parent (no more than once every configured period).

The data-rate shift can be displayed using the **debug dot11 dot11Radio 0 trace print rates** command. However, this will not show the actual data rate shift algorithm in action, only the changes in data rate. This determines the time period to scan, depending on how much the data rate was decreased.

The period should be set depending on the application. Default is 20 seconds. This delay period prevents the WMIC from constantly scanning for a better parent if, for example, the threshold is below the configured value.

The threshold sets the level at which the algorithm is triggered to scan for a better parent. This threshold should be set to *noise+20dBm* but not more than -70dBm (+70 because input for threshold is positive). The default is -70 dBm.

## Using Network Address Translation (NAT) with the MAR3200

Without the use of Mobile IP, devices connected to the MAR3200 will need to use NAT and static routing to route traffic. On the MAR3200 create a subnet for clients to connect to and NAT that subnet to the WMIC interface. For return traffic destined to devices or clients attached to the MAR3200 create static route pointing back to the MARs WMIC interface on a router connecting to the mesh WLC.

To configure NAT and static routing, refer to [Figure 10](#) and perform the following steps (assuming you already configured the WMIC Universal Bridge Client and Mesh network).

Perform the following steps from the router's global configuration mode:

---

**Step 1** Create a VLAN for MAR connected clients:

```
MR(config)# int vlan 5
MR(config-if)# ip address 10.10.10.1 255.255.255.0
```

**Step 2** Configure a DHCP pool to be used for connecting clients to the MAR:

```
MR(config)# ip dhcp pool CLIENTPOOL
MR(dhcp-config)# network 10.10.10.0 255.255.255.0
MR(dhcp-config)# default-router 10.10.10.1
MR(config)# ip dhcp excluded-address
MR(config)# ip dhcp excluded-address 10.10.10.1
```

**Step 3** Using the following commands, configure NAT for that pool so that it uses the VLAN interface for the WMIC that connects to the Mesh network:

```
MR(config)# ip nat inside source list 10 interface Vlan4 overload
!
MR(config)# access-list 10 permit 10.10.10.0 0.0.0.255 log
```

**Step 4** Label your inside and outside NAT interfaces:

```
MR(config)# interface Vlan4
MR(config-if)# ip address 10.20.42.1 255.255.255.0
MR(config-if)# ip nat outside
!
MR(config)# interface Vlan5
MR(config-if)# ip address 10.10.10.1 255.255.255.0
MR(config-if)# ip nat inside
```

**Step 5** Configure a default gateway on the MAR that points to the Mesh network:

```
MR(config)# ip default-gateway 10.20.41.1
```

**Step 6** Save the configuration on the MAR3200 and exit:

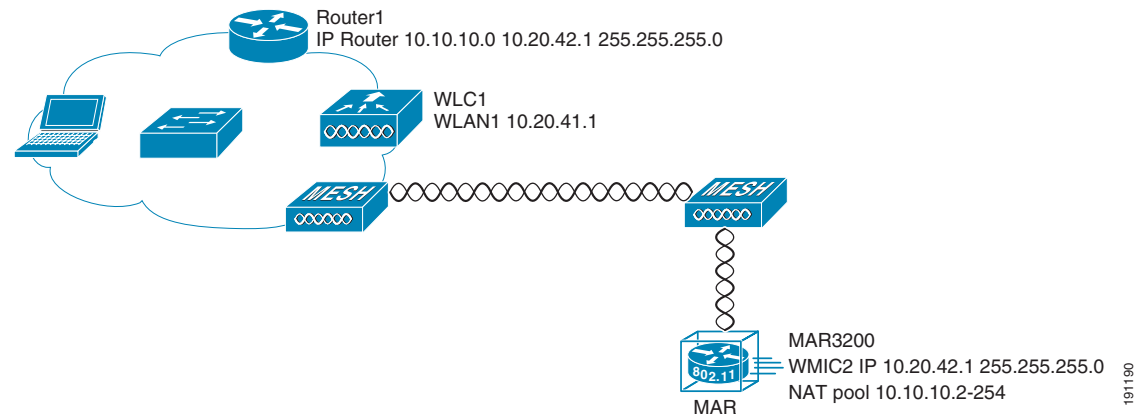
```
MR# wr mem
MR# exit
```

**Step 7** Log on to Router1 and configure static routing (see [Figure 10](#) for static routes):

```
Router1(config)# ip route destination network netmask Forwarding router's address
```

**Step 8** Save your configuration and exit:

```
Router1# write memory
Router1# exit
```

**Figure 10 NAT and Static Routing**

## MAR3200 in Mobile IP Environments

The wireless technologies used in many current metropolitan mobile networks include 802.11 wireless mesh networks for general city-wide coverage, providing high speed access for bandwidth-intensive applications, such as in-car video. For coverage areas where it is not practical to extend the wireless mesh network, it can be supplemented by cellular services, such as CDMA 1x RTT. Using this approach, cellular services can be used to fill gaps in connections and provide backup wireless connectivity. This added backup interface requires Mobile IP to enable client roaming between the two separate networks.

To enable Mobile IP, an HA router must be added to the enterprise network to tunnel client traffic between the MR and its home network. Another requirement for Mobile IP is to configure the MAR3200 as an MR. The following section describes Mobile IP registration process. [Figure 11](#) shows a simple Mobile IP (MIP) environment.

## The MAR 3200 Mobile IP Registration Process

When the MAR3200 is associated to its Mesh network, the following events occur:

- The MAR3200 goes through a Foreign Agent (FA) discovery process.  
FAs advertise their existence periodically. If a MR does not hear a FA advertisement, it solicits itself by sending a multicast advertisement to the address 224.0.0.2.
- If an FA receives a solicitation from an MR, it responds with a unicast advertisement to the MR that includes its Care of Address (CoA).
- If the access network does not have a FA router, the MR can register itself with the HA by using a Collocated Care of Address (CCoA).

The CCoA address is the IP address of the interface the MR uses to connect to the access network.

191190

- The MR then sends in Registration Request (RRQ) to the HA.
- The HA authenticates MR by sending a Registration reply (RRP) to the MR.
- The HA provides a gratuitous APR update for the home network, then creates a GRE tunnel to the FA if using Foreign Agent CoA (FACoA), or to the MR if you are using CCoA. It then adds a host route to the MR.
- Now, the MR has reached a registered state with the HA and the HA has set up a binding table entry for the MR CoA. It will then tunnel and route traffic destined for the MR.
- At this point, the MR is registered through a Mesh WLAN to its HA using the FACoA.

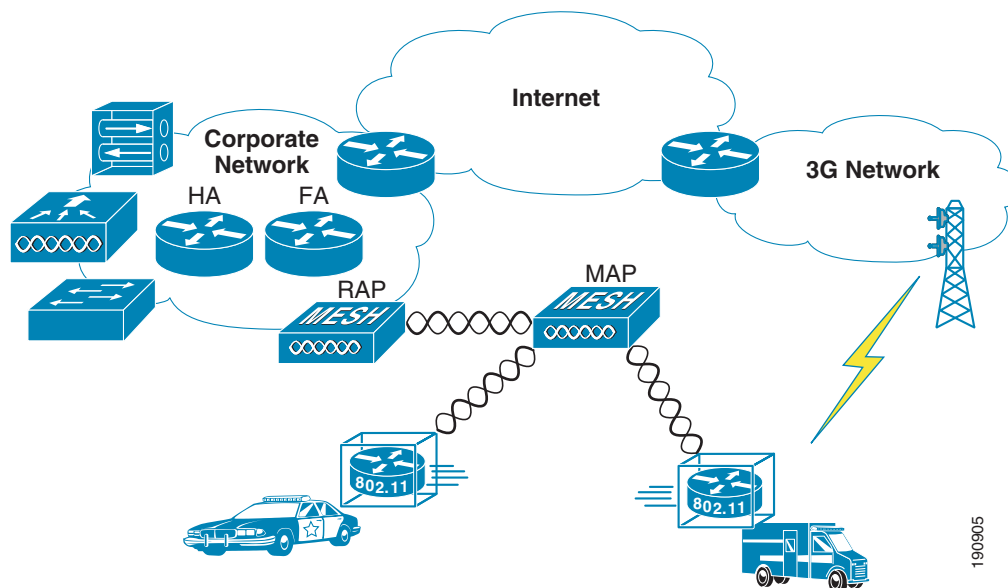
If any devices attached to the Cisco 3200 Series router must communicate with nodes on the home network, they send the data to the Cisco 3200 Series router and Mobile IP tunnels the data to the HA, with any traffic directed to MR clients tunneled from the HA to the MR. A simple Mobile IP network with FACoA for Mesh and Collocated Care of Address (CCoA) for cellular is illustrated in Figure 11.

Mobile IP is needed if your application requires routing to any devices or nodes attached to the MAR3200.

- If the MAR3200 is not in the vicinity of a wireless LAN hotspot it can use a backup wireless service such as cellular modem to deliver the data.

In this case, the Cisco 3200 generates a CCoA from the IP address it acquired from the service provider network and registers its CCoA with the HA. This CCoA address is the MR's own interface IP address it acquired via DHCP from the service provider. The registration process is similar to the process for CoA registration.

**Figure 11 Mobile IP Example**



190905

## Mobile IP Configuration

This section describes the Mobile IP configuration process.

### Basic HA and Foreign Agent Router Configurations

This configuration illustrates connecting two separate Mesh networks that have different mobility groups with Mobile IP. This enables an MR to seamlessly roam between the two networks (see [Figure 11](#)).

To configure an HA and FA router, perform the following steps:

- Step 1** Log into the HA router. This can be any Cisco router that supports the Mobile IP feature set.
- Step 2** Enable two Fast Ethernet or Gigabit Ethernet onboard interfaces which are used to connect to two foreign agent routers:

```
HA1(config)# interface GigabitEthernet 0/1
HA1(config-if)# no shut
HA1(config)# interface FastEthernet 0/1
HA1(config-if)# no shut
```

- Step 3** Configure an IP address on each interface, based on the information in [Figure 11](#):

```
HA1(config-if)# ip address network interface address netmask
```

- Step 4** Configure a loopback interface:

```
HA1(config)# interface loopback 0
HA1(config-if)# ip address network interface address netmask
```

Fast Ethernet interfaces on a switch module are for the devices behind HA. Default VLAN 1 is for the home network.

- Step 5** Log into the FA router, using the **vlan database** command in enable mode to create VLAN 2 and VLAN 3. Create a VLAN interface for each VLAN using the IP address shown in [Figure 11](#).

On the FA, VLAN 2 is used to connect to the HA router. VLAN 3 is for connection to the Mesh network.

| Connected to | Interface        | VLAN | Description                        |
|--------------|------------------|------|------------------------------------|
| HA           | FastEthernet2/0  | 2    | Wired uplink connection to HA.     |
| MESH AP      | FastEthernet 0/0 | 3    | Wired uplink connection to MESH AP |

### Configuring OSPF Routing Between HA, FA1, and FA2

To configure OSPF routing between the HA, FA1, and FA2, perform the following steps:

- Step 1** Using the following commands, configure OSPF routing between the HA and FA routers. Use area 0 between routers and include all of the networks:

```
HA1(config)# router ospf 10
HA1(config-router)# network x.x.x.x y.y.y.y area 0
```

- Step 2** Use the **show ip route** command to verify the routing table on each router. From the FA, you should be able to ping **10.10.10.1**, which is the loopback address of the HA.

## Configuring IP Address, DHCP, and VLAN on the MR

To configure the IP address, the DHCP, and the VLAN on the MR, perform the following steps:

- Step 1** Connect to and log in to the MR.
- Step 2** Create a loopback interface and assign IP address:
- ```
MR1(config)# Interface loopback 0
```
- Step 3** Create VLAN 2 in VLAN database using the **vlan database** command. Configure VLAN 1 and VLAN 2 interface. VLAN 1 is used for 2.4 GHz WMIC2 (W2) acting as AP and VLAN 2 is for 4.9GHz WMIC (W3). Configure FA2/0, FA2/1 and FA2/3 to be in VLAN 1, and FA 2/2 to be in VLAN 2.

Connected to	Interface	Radio Type	VLAN	Description
PC	FastEthernet2/0	None	1	Fast Ethernet link for end device
WMIC 1 (W1)	FastEthernet 0/0	2.4GHz	None	2.4 Ghz Wireless Universal Work Group Bridge uplink to Mesh network
WMIC 2 (W2)	FastEthernet 2/3	2.4GHz	1	Provide 2.4 GHz AP Hotspot around the MR

- Step 4** Configure the wireless client's DHCP pool:

```
MR1(config)# ip dhcp pool mypool
MR1(dhcp-config)# network 10.40.10.0 /28
MR1(dhcp-config)# default-router 10.40.10.1
MR1(dhcp-config)# ip dhcp excluded-address 10.40.10.1 10.40.10.3
```

Configuring a 2.4GHz Access Point on the MR

To configure a 2.4GHz access point on the MR, perform the following steps:

- Step 1** Connect the console cable between the PC and the console port for 2.4GHz WMIC2 (W2) and log into it using the default password.
- Step 2** Configure the IP address on BVI interface and the default gateway. Verify the management connection between WMIC and MARC:

```
MR1(config-if)# ip address network interface address netmask
MR1(config-if)# exit
MR1(config)# ip default-gateway address of default gateway
MR1(config)# exit
MR1# show ip interface brief
```

- Step 3** Configure radio interface to have AP station role and SSID home pod#:

```
MR1(config)# interface Dot11Radio0
MR1(config-if)# ssid home pod#
MR1(config-if)# authentication open
MR1(config-if)# channel 6
```

```
MR1(config-if)# station-role root ap-only
```

Authentication or static WEP key configuration is optional. Remove the default SSID and select a non-overlapping channel that is different from the one selected in Step 2.

Configuring the 2.4 Universal Work Group Bridge Client

To configure the Universal Work Group Bridge Client, perform the following steps (from global configuration mode):

- Step 1** Connect the console cable between PC and the console port for 2.4GHz WMIC1 (W1) on FA1 and log into it using default password.
- Step 2** Configure the IP address on BVI interface and the default gateway based on diagram. Verify the management connection between WMIC and MARC.
- Step 3** Configure radio interface to have root station role and SSID metro *pod#_bridge*. Remove the default SSID. Use open authentication and WPA share key:

```
MR1(config)# interface Dot11Radio0
MR1(config-if# encryption mode ciphers tkip
MR1(config-if# ssid MobileMESH
MR1(config-if# authentication open
MR1(config-if# authentication key-management wpa
MR1(config-if# infrastructure-ssid
MR1(config-if# wpa-psk ascii ciscocisco
MR1(config-if# station-role workgroup-bridge universal mac address
```



Note

Refer to [Universal Workgroup Bridge Considerations, page 7](#) and [WMIC Universal Bridge Client Configuration, page 12](#) for more information regarding Universal Work Group Bridge and configuration options.

- Step 4** Connect to the WLAN controller and configure WLAN1 to use WPA-PSK with the same settings you configured in Step 3.
- Step 5** Verify the wireless connection between UWGB and MESH. Use the **show dot1 association** command on the MR to verify the association status. Ping the WLC management interface address across the wireless link.

Configuring the Home Agent (HA)

The MR in the lab will host different IP networks. Use the entries in the following table to configure the HA, FA, and MR.

Cisco 3200 Mobile Router	Mobile Router Loopback Address	SPI	SPI Key Hex String	Mobile Networks	Mobile Router FE 0/0 Address	WMIC Workgroup Bridge IP Address	VLAN1 and PC IP Address
1	10.20.10.1	100	1234567812345678 1234567812345678	10.30.10.0/28 10.40.10.0/28	10.30.10.1	10.30.10.2	10.40.10.1 10.40.10.0/28
2	10.20.10.2	200	2345678123456781 2345678123456781	10.30.10.16/28 10.40.10.16/28	10.30.10.17	10.30.10.18	10.40.10.17 10.40.10.16/28

Perform the following steps to configure the HA router:

-
- Step 1** Log into the HA router. To determine the current configuration of the HA, enter either of these commands:
- ```
HA# show ip mobile globals
HA# show running-configure
```
- Step 2** Enable Mobile IP and configure the router as HA. Specify **10.20.10.0** as the virtual home network.
- Step 3** to enter the Mobile IP mode, enter:
- ```
HA(config)# router mobile
```
- Step 4** To specify that this is an HA, enter:
- ```
HA(config)# ip mobile home-agent
```
- Step 5** To create the virtual network, enter:
- ```
HA(config)# ip mobile virtual-network 10.20.10.0 255.255.255.0
```
- Step 6** Configure IP mobile-related parameters for IP mobile host, network and authentication. Refer to the table for the variable information, such as the IP addresses and IP networks. Redistribute the mobile routes into OSPF routing.
- To create the mobile host for the MR, enter:


```
HA(config)# ip mobile host mobile router loopback address from the table
virtual-network 10.20.10.0 255.255.255.0
```
 - To specify networks on this MR, enter:


```
HA(config)# ip mobile mobile-networks mobile router loopback address from the table
```
 - To configure the first network for this router, enter:


```
HA(config-router)# network mobile router network from the table 255.255.255.240
```
 - To configure the second network for this router, enter:


```
HA(config-router)# network mobile router network from the table 255.255.255.240
```
 - Enter:


```
HA(config)# ip mobile secure host mobile router loopback address spi SPI number from
table key hex string from table
```


- f. To enter route protocol mode, enter:

```
HA(config)# router ospf 10
```

- g. Enter:

```
HA(config-router)# redistribute mobile subnets
```

- Step 7** To verify your configuration, enter:

```
HA# show run
```

```
HA# show ip mobile globals
```



Note

The AAA server can be used to hold all MR spi and key. The command for this is **ip mobile host *mobile router loopback address from table* virtual-network 10.20.10.0 255.255.255.0 aaa load-sa**. The **load-sa** keyword instructs the HA to hold the security association (SPI/Key) in memory for subsequent registrations. Additionally, you can enter a range of MR hosts in the command.

Networks on the MR can also dynamically register to the HA besides statically configuring networks under ip mobile mobile networks. The command to do this on the HA is **ip mobile mobile-network *mobile host* register**.

Configuring the Foreign Agent (FA)

The Foreign Agent does not need a specific configuration for each MR and its IP addresses. All that is required is to activate the FA features on the router. The Mobile IP configurations are the same for two FA routers. The following steps are required to enable the Mobile IP foreign agent service.

- Step 1** Log into the FA router.

- Step 2** Enter either of the following commands to determine the configuration on each FA router:

```
FA# show ip mobile globals
```

```
FA# show running-configure
```

- Step 3** Enable MoIP on the FA router. Specify the VLAN 3 interface as care-of address. (COA), which is connected to 4.9GHz bridge WMIC:

```
FA# router mobile
```

```
FA# ip mobile foreign-agent care-of vlan 3
```

- Step 4** Enable IRDP and MoIP foreign-service on the VLAN 3 interface using following commands:

```
FA(config)# interface vlan 3
```

```
FA(config-if)# ip irdp
```

```
FA(config-if)# ip irdp minadvertinterval 3
```

```
FA(config-if)# ip irdp maxadvertinterval 4
```

```
FA(config-if)# ip irdp holdtime 13 must be > 3 X Max interval
```

```
FA(config-if)# ip mobile foreign-service
```


- Step 5** To verify your configuration, enter:

```
FA# show run
```

```
FA# show ip mobile globals
```

Configuring the Mobile Router (MR)

Perform the following steps to configure the MAR as a MR for use in a Mobile IP network:

-
- Step 1** Log in to the MR.
- Step 2** Enter either of the following commands to determine the current configuration of the MR:
- ```
MR# show ip mobile globals
MR# show running-configure
```
- Step 3** Enable MoIP on the MR. Enable mobile route and configure the MoIP variable globally including HA information. From the router's global configuration mode, enter the following commands:
- ```
MR(config)# router mobile
MR(config)# ip mobile router
MR(mobile-router)# address mobile router loopback address 255.255.255.255
MR(mobile-router)# home-agent 10.10.10.1
```
- Enter the **exit** command to exit from Mobile Router mode.
- Enter:
- ```
MR(config)#ip mobile secure home-agent 10.10.10.1 spi SPI number from table key hex string
from table
```
- 
- Note** The SPI number and string must match those you entered for the HA exactly or the tunnel and the mobile connection will not come up.
- 
- Step 4** Enable MoIP on MR. Enable mobile route and configure MoIP variable globally including HA information:
- ```
MR(config)# interface vlan 2
MR(config-if)#ip mobile router-service roam
MR(config-if)#ip mobile router-service solicit interval 5
```
- Step 5** Enter the **show ip mobile router** command to verify your configuration.
-

Verifying the Mobile IP Configuration

To verify the Mobile IP configuration, perform the following steps from the MR:

-
- Step 1** To view the advertisements from the FAs, enter:
- ```
MR# debug ip icmp
```
- Step 2** To verify that your MR is receiving advertisements from one FA, enter:
- ```
MR# show ip mobile router agent
```
- Is your MR sending IRDP solicitations?
- Step 3** To verify that the MR has associated with the HA, and that the tunnels are up, enter:
- ```
MR# show ip mobile router
```
- Step 4** Log into that FA and examine the operation of the FA using the following commands:
- ```
FA# show ip mobile global
```

```
FA# show ip mobile interface
FA# show ip mobile visitor
FA# show ip route
```

What do you see as the interface to the routes on the MR?

Step 5 Log into the MR and verify that the routes to the HA are there:

```
MR# show ip route
```

Step 6 To verify that traffic is being passed, enter:

```
MR# show ip mobile router traffic
```

Step 7 Enter:

```
MR# debug ip mobile router
```

Step 8 Enter the following command and monitor the output:

```
MR# clear ip mobile router registers
```

Step 9 Connect your laptop to the network behind the MR. You should also be able to ping the PCs behind the HA router continuously.

Step 10 Log into the HA and examine its operation using the following commands:

```
HA# show ip mobile global
HA# show ip mobile mobile-networks
HA# show ip mobile host
HA# show ip mobile secure host
HA# show ip route
```

For more information on Mobile IP, refer to the following URL:

http://www.cisco.com/en/US/tech/tk827/tk369/tk425/tsd_technology_support_sub-protocol_home.html.

