



## Mobile Access Router, Universal Bridge Client, and Cisco Unified Wireless

The Cisco 3200 Series Mobile Access router (also referred to as the MAR3200) is a compact, high-performance access solution that offers seamless mobility and interoperability across wireless networks. The size of the Cisco MAR3200 (see [Figure 13-1](#)) makes it ideal for use in vehicles in public safety, homeland security, and transportation sectors. The MAR3200 delivers seamless communications 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.

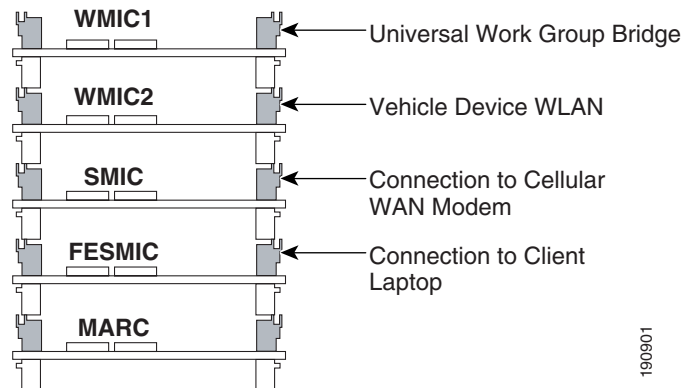
**Figure 13-1** Cisco 3200 Series Mobile Access Router



## 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*. It 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)). Figure 13-2 shows this stackable card configuration. The router can also be configured in a rugged enclosure with power adapters.

**Figure 13-2 Card Connections**

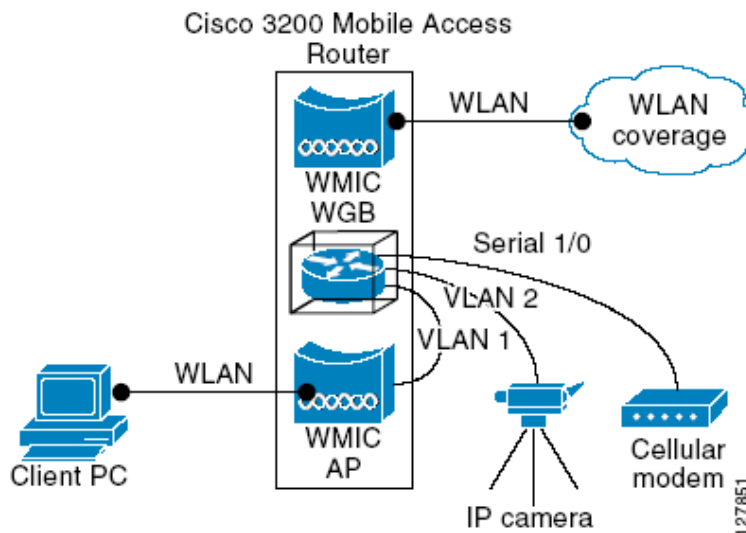


For more information on MAR3200 configuration options, see the following URL:

[http://www.cisco.com/en/US/products/hw/routers/ps272/products\\_data\\_sheet0900aecd800fe973.html](http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd800fe973.html)

Figure 13-3 provides an example of a MAR3200 configured with two WMICs, an FESMIC, and a MARC.

**Figure 13-3 Mobile Unit Configuration Example**



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

Table 13-1 shows the setup of WMICs on the Cisco 3230 Mobile Access router.

**Table 13-1 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 13-2 shows the setup of serial interfaces on the Cisco 3230 Mobile Access router.

**Table 13-2 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 13-3 shows the setup of Fast Ethernet interfaces on the Cisco 3230 Mobile Access router.

**Table 13-3 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 13-4 highlights the software features of WMICs running Cisco IOS.

**Table 13-4 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"> <li>• WEP keys: Message Integrity Check (MIC) and WEP key hashing CKIP</li> <li>• WPA</li> <li>• WPA2</li> </ul>
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.
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 13-5](#) lists the supported features.

**Table 13-5 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
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	

**Table 13-5 CCX Version Feature Support (continued)**

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.

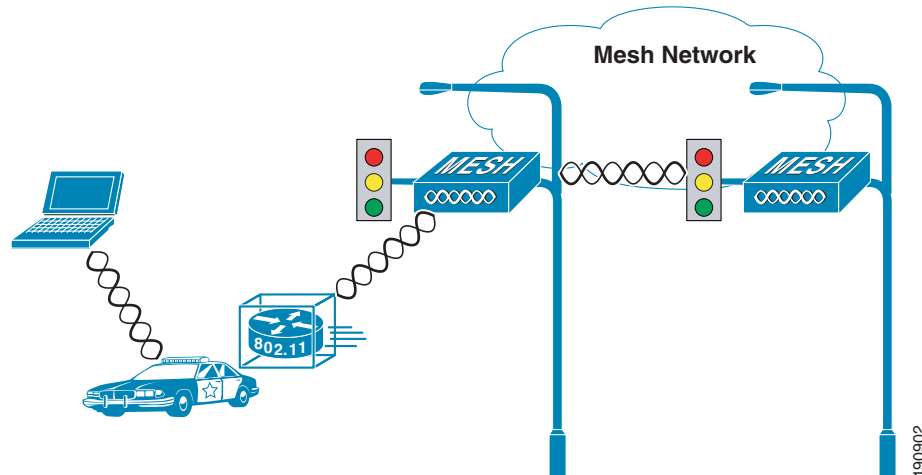
## Vehicle Network Example

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 13-4](#) 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 13-4 Vehicle Network Example**



## Simple Universal Bridge Client Data Path Example

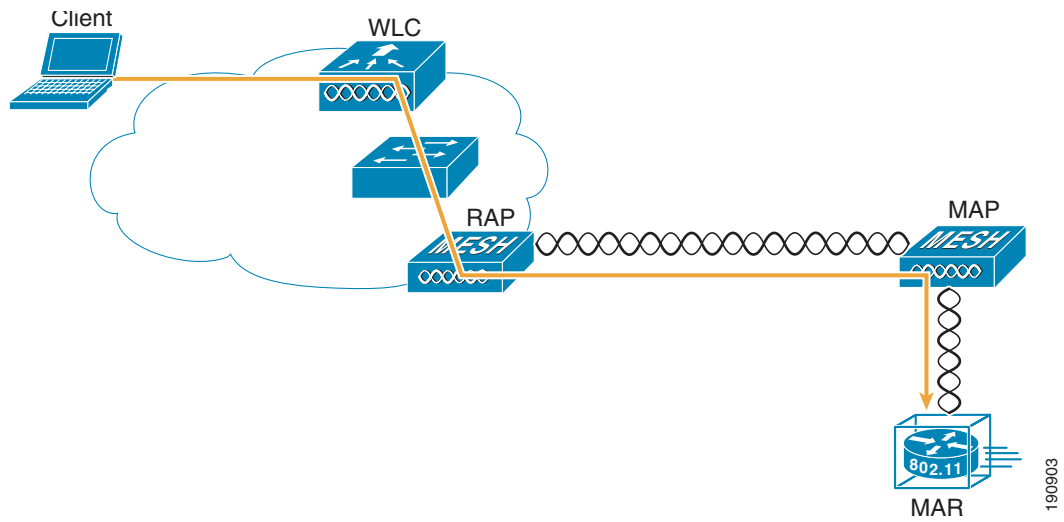
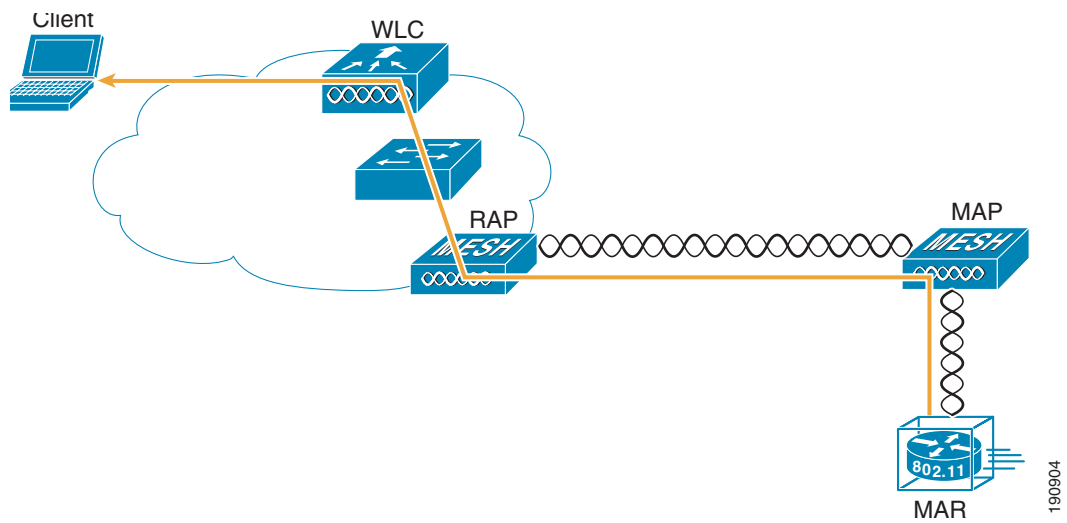
The IP devices connected to the MAR are not *aware* that they are part of a mobile network. When they must communicate with another node in the network, their traffic is sent to their default gateway, the Cisco 3200 Series router. The Cisco 3200 Series router forwards the traffic to the Mesh APs WLAN,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

As shown in [Figure 13-5](#), 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 13-6](#) shows the return path to the MAR. Mobile IP eliminates the need for static routing and will be discussed further in this chapter. NAT may be used in simple deployments when Mobile IP is not available.

The data path example shown in [Figure 13-5](#), 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 will be 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 13-5 Simple Layer 2 Data Path Example****Figure 13-6 Client Return Data Path**

## Configuration

The following is a configuration example for the MAR3200. It can be used as a step-by-step process to configure the Universal Work Group Bridge client using open authentication, and WEP encryption. It also covers other basic configuration steps such as VLAN creation, assignment, and DHCP.

### Connecting 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 female). Use a straight through DB9-to-DB9 cable.



#### Note

You can also use the same console cable used to access the HA, with the addition of an RJ-45 to DB9 female adapter.

### Configuring the IP Address, DHCP, VLAN on MAR

- Step 1** Connect to and log into the Mobile Router.
- Step 2** Create a loopback interface and assign an IP address.
- Step 3** Create VLAN 2 in the VLAN database using the **vlan database** command.
- Step 4** 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 5** Create VLAN 4 in the VLAN database for connection between WMIC 1 and MARC.

**Table 13-6**

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 mobile router
WMIC 3 (W3)	FastEthernet2/2	4.9GHz	2	4.9GHz uplink as Workgroup Bridge

- Step 6** Configure DHCP server for VLAN 3 using following commands:  

```
ip dhcp pool mypool
network 10.40.10.0 /28
default-router 10.40.10.1
ip dhcp excluded-address 10.40.10.1 10.40.10.3
```
- Step 7** Verify that the wired client on VLAN 3 has been assigned a DHCP IP address in the **10.40.10.0/28** subnet.

## Configuring the Universal Bridge Client on WMIC

This configuration is made on the WMIC, and is used for connecting the Mobile Access router (MAR) to a Cisco Mesh network.

---

**Step 1** Configure the SSID of the mesh network on the MARs WMIC with which you plan to connect.

**Step 2** Connect to the console port of the WMIC:

**dot11 ssid (A given SSID)**

**Step 3** Configure your authentication type:

**authentication (Auth Type)**

**client EAP client information**

**key-management key management**

**network-eap leap method**

**open open method**

**shared shared method**

**Step 4** Configure your encryption key, if needed:

**encryption key 1 size 128bit 7 FA1E467E23EAD518A21653687A42 transmit-key**

**encryption mode wep mandatory**

**Step 5** Configure the WMIC to act as a universal client to the Mesh network:

**station-role workgroup-bridge universal (mac address)**




---

**Note** You must use the MAC address of the associated VLAN that the WMIC is bridged to. For example, to use the MAC address of VLAN 1, acquire the MAC address of VLAN 1 by entering the **show mac-address-table** command from the console of the MARs router card.)

---

**Step 6** Bridge the dot11 interface:

**bridge-group 1**

**bridge-group 1 spanning-disabled**

**Step 7** Bridge the ethernet interface:

**FastEthernet0**

**bridge-group 1**

**Step 8** Configure the bridged virtual interface:

**interface BVI1**

**no ip address**

**no ip route-cache**

## Configuring the MARs Router Card

The following configuration is for the router card of the MAR.

- 
- Step 1** Find the interface the WMIC is associated with by issuing the following command:
- show CDP neighbors!**
- Step 2** Configure the interface with the matching VLAN that you used in Step 5 for the MAC address in the universal client command:
- interface FastEthernet2/2**  
**switchport access vlan 4**
- Step 3** Configure the VLAN to use DHCP if you are going to be using DHCP on the MAR:
- interface Vlan4**  
**ip address dhcp**
- 

## WMIC Roaming Algorithm

Four basic triggers start the WMIC scanning for a better root bridge or access point:

- The loss of eight consecutive beacons
- The data rate shifts
- 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.

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

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

If mobile station is configured. 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 with 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 since input for threshold is positive). The default is -70 dBm.

## MAR3200 in a 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, a Home Agent (HA) router must be added to the enterprise network to tunnel client traffic between the Mobile Router and its home network. Another requirement for Mobile IP is to configure the MAR3200 as a Mobile Router (MR). The following section describes Mobile IP registration process. [Figure 13-5](#) displays a very simple Mobile IP (MIP) environment.

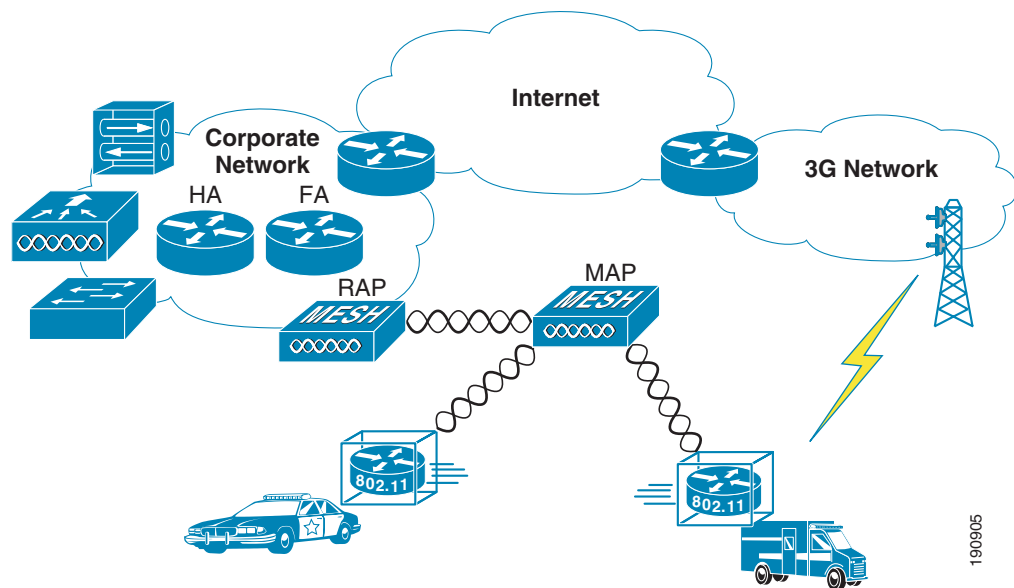
## MAR 3200 Mobile IP Registration Process

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.
- 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 mobile router is registered through a Mesh WLAN to its HA using the FCoA.  
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 FCoA for Mesh and Collocated Care of Address (CCoA) for cellular is illustrated in [Figure 13-7](#). 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 hot spot 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 home agent. This CCoA address is the mobile router'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 13-7 Mobile IP Example**



For more information on Mobile IP, see the following URL:

[http://www.cisco.com/en/US/tech/tk827/tk369/tk425/tsd\\_technology\\_support\\_sub-protocol\\_home.html](http://www.cisco.com/en/US/tech/tk827/tk369/tk425/tsd_technology_support_sub-protocol_home.html)

