Configuring the WMIC for the First Time

This chapter describes how to configure basic settings on a Wireless Mobile Interface Card (WMIC) for the first time. You can use the command line interface (CLI) to configure all the settings described in this chapter.

Before You Start

Before you install the WMIC, make sure that you are using a computer connected to the same network as the WMIC, and obtain the following information from your network administrator:

- A system name for the WMIC
- The case-sensitive wireless service set identifier (SSID)
- If not connected to a DHCP server, a unique IP address for the WMIC (such as 172.17.255.115)
- If the WMIC is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)

Connecting to the WMIC

To configure the WMIC:

- Connect a PC to the WMIC console port by using the console cable.
- If the WMIC has an IP address and Telnet is allowed on the device, you can connect to the Fast Ethernet Switch Mobile Interface Card (FESMIC) Ethernet port by using an Ethernet cable, and by using Telnet to establish the connection.
- If the WMIC is on a LAN and has an IP address, and if Telnet is allowed on the device, you can telnet into the WMIC from a node on the LAN.

Note When you connect your PC to the WMIC or reconnect your PC to the LAN, it might be necessary to release and renew the IP address on the PC. On most PCs, you can release and renew the IP address by rebooting the PC or by entering the **ipconfig /release** and **ipconfig /renew** commands in a command window. Consult your PC documentation for detailed instructions.

Using the Console Port to Access the Privileged Exec Mode

Connect a PC to the WMIC console port by using a DB-9-to-RJ-45 serial cable. Note that there might be several console ports on a Cisco 3200 Series router.

Follow these steps to connect a PC to the WMIC console port and access the CLI:

Step 1 Connect the RJ-45 end of a DB-9-to-RJ-45 serial cable to the WMIC RJ-45 serial port on the router.

Step 2 Connect the DB-9 end of the DB-9-to-RJ-45 serial cable to the to the COM port on your PC.

Step 3 Start a terminal emulator application to communicate with the WMIC. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. When the terminal emulator establishes communications, a router prompt displays.

Step 4 Press **Enter**. A prompt appears.

Step 5 Type **en**. A prompt for the username appears.

Step 6 Enter the *username*. The default username is *Cisco*. The password prompt displays.

Step 7 Enter the WMIC password. The default password is *Cisco*.

A prompt displays, indicating that you are in *Exec* mode.

Using a Telnet Session to Access the Privileged Exec Mode

Follow these steps to access the WMIC CLI by using a Telnet session. The WMIC must have been previously configured to accept a Telnet session.

These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your computer documentation for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**. If Telnet is not listed in the Accessories menu, select **Start > Run**, type **Telnet** in the **Open** field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the WMIC IP address.

Step 3 In the Host Name field, type the WMIC IP address and click **Connect**.

Opening the CLI with Secure Shell

Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. It provides more security for remote connections than Telnet. See the "Configuring the WMIC for Secure Shell" section for instructions on setting up the WMIC for SSH access. (For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/)

Obtaining and Assigning an IP Address

Assign the WMIC IP address by using one of the following methods:

- Use the console when you connect to the WMIC locally. For detailed instructions, see the "Connecting to the WMIC" section on page 2-1.
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address by doing one of the following:
  - Provide your organization's network administrator with the WMIC Media Access Control (MAC) address. The network administrator will query the DHCP server using the MAC address to identify the IP address.
  - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. You can also use IPSU to assign an IP address to the WMIC if it did not receive an IP address from the DHCP server. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, ME, NT, and XP.

    You can download IPSU from the Software Center on Cisco.com. Click this link to browse to the Software Center:

    http://www.cisco.com/public/sw-center/sw-wireless.shtml
  - If the unit is a non-root bridge, connect to the WMIC console port of the router locally.

Assigning an IP Address By Using the Exec

The WMIC links to the network by using a Bridge Group Virtual Interface (BVI) that it creates automatically. Each WMIC supports one BVI. Configuring more than one BVI might cause errors in the WMIC Address Resolution Protocol (ARP) table.

Beginning in privileged EXEC mode, follow these steps to assign an IP address to the BVI:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface bvi1**	Enter interface configuration mode for the BVI.
Step 3	**ip address** *address subnetmask*	Assign an IP address and subnet mask to the BVI. **Note** If you are connected to the WMIC using a Telnet session, the connection to the WMIC will go down when you assign a new IP address to the BVI. To continue configuring the WMIC by using Telnet, use the new IP address to open another Telnet session to the WMIC.

Protecting Your Wireless LAN

After you assign basic settings to your WMIC, you need to configure security settings to prevent unauthorized access to your network. Because it is a radio device, the WMIC can communicate beyond the physical boundaries of a building. Advanced security features are described in the following chapters:

- A unique SSID that is not broadcast in the beacon (see Chapter 5, “Configuring SSIDs”)
- Wired Equivalent Privacy (WEP) and WEP features (see Chapter 8, “Configuring Cipher Suites and WEP”)
- Dynamic WEP and WMIC authentication (see Chapter 9, “Configuring Authentication Types”)

Configuring Basic Security Settings

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your worksite.

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Express Security Types

Table 2-1 describes the four security types that you can assign to an SSID.

Table 2-1 Security Types on Express Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs that are used in a public space. Assign this option to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the access point based on MAC address, or, if your network does not have a RADIUS server, consider using an access point as a local authentication server.	Mandatory WEP encryption, no key management, and open authentication. In **Root AP** mode, client devices cannot associate by using this SSID without a WEP key that matches the access point key.
EAP Authentication	This option enables 802.1x extensible authentication protocol (EAP) types, including Lightweight EAP (LEAP), Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS), and EAP-GTC, and requires you to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1x authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1x authentication. In **Root AP** mode, client devices that associate by using this SSID must perform 802.1x authentication.
WPA	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, and then encrypts their IP traffic with stronger algorithms than those used in WEP. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. In **Root AP** mode, client devices that associate by using this SSID must be WPA-capable.

CLI Security Configuration Examples

This section provides example configurations for creating SSIDs and assigning security.

Example: No Security

This example shows part of the configuration that results from using the Express Security page to create an SSID called *no_security_ssid*, including the SSID in the beacon, assigning it to VLAN 10, and selecting VLAN 10 as the native VLAN:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid no_security-ssid
    vlan 10
    authentication open
    guest-mode
 !
!
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
 bridge-group 10 spanning-disabled
!
interface FastEthernet0.10
encapsulation dot1Q 10
no ip address
no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```

Example: Static WEP

This example shows part of the configuration that is used to create an SSID called *static_wep_ssid*, excluding the SSID from the beacon, assigning the SSID to VLAN 20, selecting 3 as the key slot, and specifying a 128-bit key:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 20 key 3 size 128bit 7 4E78330C1A841439656A9323F25A transmit-ke
y
 encryption vlan 20 mode wep mandatory
 !
 ssid static_wep_ssid
    vlan 20
    authentication open
 !
 concatenation
```

```
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
```

Example: EAP Authentication

This example shows part of the configuration that is used to create an SSID called *eap_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 30:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
    vlan 30
    authentication open eap eap_methods
    authentication network-eap eap_methods
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
```

```
interface FastEthernet0
 mtu 1500
 no ip address
 ip mtu 1564
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.30
 mtu 1500
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
```

Example: WPA

This example shows part of the configuration that is used to create an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```
aaa new-model
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 40 mode ciphers tkip
 !
```

```
 ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
 !
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/122-15.JA/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 135445415F59
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
line con 0
line vty 5 15
!
end
```