Cisco 3200 Series Mobile Access Router Interfaces

The Cisco 3200 Series routers can be configured through the console ports.

The following topics are described:

- Terminal Configuration
- Command Line Interface Basics
- Basic Mobile Access Router Interface Configuration
- Remote Access to the Router

The physical characteristics of the router console interface are described in the Cisco 3200 Series Mobile Access Router Hardware Reference.

For descriptions of configuration commands and the configuration options available, refer to the appropriate software publications listed in the "Related Documentation" section.

Timesaver Before you begin, disconnect all WAN cables from the router to keep it from trying to run the AutoInstall process. The router tries to run AutoInstall whenever you power it on, if there is a WAN connection on both ends and the router does not have a valid configuration file stored in nonvolatile random-access memory (NVRAM) (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote Transmission Control Protocol/Internet Protocol (TCP/IP) host.

Terminal Configuration

To configure the router by using a terminal, make sure you configure the terminal to match the router console port as follows:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit

Command Line Interface Basics

The command–line interface (CLI) can be used to set the parameters for the Cisco IOS software loaded on the router. Because the CLI is divided into different modes, the commands available to you at any given time depends on which mode you are in. Each mode is indicated by the prompt. Entering a question mark (**?**) at the CLI prompt displays a list of available commands.

Command-Line Modes

When you log in to the CLI, you are in *User EXEC* mode. User EXEC mode allows monitoring of the router, but few of the commands available in this mode allow modification of the configuration. To modify the configuration, you must enter *Privileged EXEC* or *Enable* mode. From Privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can change to *global configuration* mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

Configuration modes allow you to make changes to the running configuration; the parameters that govern the behavior of the router. If you save the *running configuration* to the *startup configuration*, the command parameters are stored in a file in the router memory and executed when the router is powered on or rebooted.

If the router cannot successfully load an Cisco IOS, it displays ROM monitor (ROMMON) mode. A user can also choose to enter ROMMON mode. ROM monitor is described in the "Access ROM Monitor Mode" section in the"Troubleshooting the Cisco 3200 Series Mobile Access Router" chapter.

Table 2-1 describes how to enter and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 2-1 Entering and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command, or press **Ctrl-Z**.
Interface configuration	From global configuration mode, specify an interface, using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command, or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Abbreviating Commands

You have to enter only enough characters for the Cisco IOS to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
Router# show conf
```

Command-Line Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Finding Command Options

The command syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space.

The Cisco IOS software displays a list and brief description of keywords and arguments available for a command. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip**

routing command; to enable IP routing after it has been disabled manually, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

command | {**begin** | **include** | **exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
Router# show interface | include protocol

FastEthernet1/0 is up, line protocol is up
Serial1/0 is up, line protocol is up
Serial1/1 is up, line protocol is up
Serial1/2 is administratively down, line protocol is down
Serial1/3 is administratively down, line protocol is down
```

For more information on the search and filter functionality, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

CLI Error Messages

Table 2-2 lists some error messages that you might encounter while using the CLI.

Table 2-2 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for the device to recognize the command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at ‘^’ marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Command History Buffer

The Cisco IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs.

By default, the router records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the Cisco IOS records during the current terminal session:

```
BR# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the Cisco IOS records for all sessions on a particular line:

```
BR(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 2-3:

Table 2-3 Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the **terminal history** global configuration command and **history** line configuration command.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Router# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Router(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Router(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 2-4 shows the keystrokes that you need to edit command lines.

Table 2-4 Editing Commands Through Keystrokes

Capability	Keystroke[1]	Purpose
Move around the command line to make changes or corrections.	**Ctrl-B** or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The Cisco IOS provides a buffer with the last ten items that you deleted.	**Ctrl-Y**	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	

Table 2-4 Editing Commands Through Keystrokes (continued)

Capability	Keystroke[1]	Purpose
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The `More` prompt appears for output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the `More` prompt.	**Return**	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the Cisco IOS suddenly sends a message to your screen.	**Ctrl-L** or **Ctrl-R**	Redisplay the current command line.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
BR(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
BR(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
BR(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
BR(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
BR(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the "Editing Commands Through Keystrokes" section on page 2-7.

Host Name and Password Configuration

Configuring a host name allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

	Command	Purpose
Step 1	Router> **enable** Password: *password* Router#	Enter enable mode. Enter the password. (The password prompt displays only if a password is configured.) You have entered enable or privileged EXEC mode when the prompt changes to Router#.
Step 2	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter global configuration mode. You have entered global configuration mode when the prompt changes to Router(config)#.
Step 3	Router(config)# **hostname** *router* Router(config)#	Change the name of the router to a meaningful name. Substitute your host name for *router*.
Step 4	Router(config)# **enable secret** *guessme*	Enter an enable secret password. This password limits access to the privileged EXEC mode. When a user types **enable** at the EXEC prompt (Router>) and an enable secret password is configured, they must enter the enable secret password to gain access to configuration mode. Substitute your enable secret for *guessme*.
Step 5	Router(config)# **line con 0**	Enter line configuration mode to configure the console port. When you enter.line configuration mode.
	Router(config-line)# **exec-timeout 0 0**	Prevent the router's EXEC facility from timing out if you do not type any information on the console screen for an extended period.
	Router(config-line)# **exit** Router(config)#	Exit back to global configuration mode.

Verifying the Host Name and Password

To verify that you configured the host name and password:

Step 1 Enter the **show config** command:

```
Router# show config
Using 1888 out of 126968 bytes
!
version XX.X
.
!
hostname Router
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
```

Check the host name and encrypted password displayed near the top of the command output.

Step 2 Exit global configuration mode and attempt to re-enter it using the new enable password:

```
Router# exit
.
Router con0 is now available
Press RETURN to get started.
Router> enable
Password: guessme
Router#
```

If you are having trouble, check the following:

- **Caps Lock** is off.
- You entered the correct passwords. Passwords are case sensitive.

Enable Mobile Access Router Services

To enable mobile access router services on the Cisco 3200 Series router, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`router mobile`**	Enables Mobile IP on the router.
Step 2	`Router(config)#` **`ip mobile router`**	Enables the mobile access router and enters mobile access router configuration mode.
Step 3	`Router(mobile-router)#` **`address`** *`ipaddress mask`*	Sets the home IP address and network mask of the mobile access router.
Step 4	`Router(mobile-router)#` **`home-agent`** *`ip-address`*	Specifies the home agent that the mobile access router uses during registration.
Step 5	`Router(mobile-router)#` **`register`** {**`extend expire`** *`seconds`* **`retry`** *`number`* **`interval`** *`seconds`* | **`lifetime`** *`seconds`* | **`retransmit initial`** *`milliseconds`* **`maximum`** *`milliseconds`* **`retry`** *`number`*}	(Optional) Controls the registration parameters of the mobile access router.
Step 6	`Router(mobile-router)#` **`reverse-tunnel`**	(Optional) Enables the reverse tunnel function.

	Command	Purpose
Step 7	`Router(mobile-router)#` **`exit`**	Exits mobile access router configuration mode.
Step 8	`Router(config)#` **`ip mobile secure home-agent`** *`address`* `{`**`inbound-spi`** *`spi-in`* **`outbound-spi`** *`spi-out`* `|` **`spi`** *`spi`*`}` **`key hex`** *`string`*	Sets up home agent security associations. The address is the home IP address of the home agent.
Step 9	`Router(config)#` **`interface`** *`type number`*	Enters interface configuration mode for the interface specified.
Step 10	`Router(config-ip)#` **`ip address`** *`ip-address mask`*	Sets an IP address for the interface.
Step 11	`Router(config-if)#` **`ip mobile router-service`** `{`**`hold-down`** *`seconds`* `|` **`roam`** `[`**`priority`** *`value`*`] |` **`solicit`** `[`**`interval`** *`seconds`*`] [`**`retransmit initial`** *`min`* **`maximum`** *`seconds`* **`retry`** *`number`*`]}`	Enables mobile access router services, such as roaming, on an interface.

Display the WMIC MAC Address

In Enable mode, you can display the MAC address by issuing a **show interface dot11Radio 0** command. For example:

```
wmic-uut#sh int dot11Radio 0
Dot11Radio0 is up, line protocol is up
  Hardware is 802.11G Radio, address is 0005.9a3e.a91a (bia 0005.9a3e.a91a)
  MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

The MAC address is displayed as the **Hardware is 802.11G Radio** parameter.

The MAC address is also displayed when the reload command is issued. For example:

```
Router#reload

System configuration has been modified. Save? [yes/no]: yes
Proceed with reload? [confirm]
Radio system: delayed or multiple reload request, ignored
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:02:31.770: %SYS-5-RELOAD: Reload requested by console.Xmodem
file system is available.
flashfs[0]: 136 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 8169984
flashfs[0]: Bytes available: 7828992
flashfs[0]: flashfs fsck took 34 seconds.
Base ethernet MAC Address: 00:05:9a:3d:32:01
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
```

The MAC address is displayed as the **Base ethernet MAC Address** parameter.

Display the Mobile Access Router Configuration

To verify the mobile access router configuration, use any of the following commands in EXEC mode:

Command	Description
`Router#` **`show ip mobile globals`**	Displays global information for mobile agents.
`Router#` **`show ip mobile mobile-networks`** [*`address`*]	Displays a list of mobile networks associated with the mobile access router.
`Router#` **`show ip mobile host`** [*`address`*]	Displays mobile node information.
`Router#` **`show ip mobile secure host`** [*`address`*]	Displays the mobility security associations for the mobile host.
`Router#` **`show ip mobile interface`**	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
`Router#` **`show ip mobile router`**	Displays configuration information and monitoring statistics for the mobile access router.
`Router#` **`show ip mobile router traffic`**	Displays the counters that the mobile access router maintains.
`Router#` **`show ip route mobile`**	Displays information about the agents for the mobile access router.
`Router#` **`show ip mobile router interface`**	Displays information about the interface that the mobile access router is using for roaming.
`Router#` **`show ip mobile router registration`**	Displays the pending and accepted registrations of the mobile access router and clear the counters.
`Router#` **`debug ip mobile router`** [**`detail`**]	Displays debug messages for the mobile access router.

Configuration File Save

Use the **copy system:running-config nvram:startup-config** command to save your running configuration to the startup configuration. The startup configuration contains all the parameters under which the router is operating. However, the startup configuration is in DRAM. If the router reloads the software or a power outage occurs, the running configuration is erased.

The startup configuration is stored in NVRAM. When the router is reloaded or powered on, the startup configuration file is copied to the running configuration file. By saving the changes to the startup configuration, your configuration parameters will not be lost.

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

To prevent the loss of the router configuration, save it to NVRAM.

	Command	Purpose
Step 1	Router> **enable** Password: *password* Router#	Enters enable mode. Enter the password. You have entered enable mode when the prompt changes to Router#.
Step 2	Router# **copy running-config startup-config**	Copies the running configuration file to the startup configuration file in NVRAM.
Step 3	Router(config-if)# **Ctrl-z** Router# %SYS-5-CONFIG_I: Configured from console by console	Returns to enable mode. This message is normal and does not indicate an error.

Basic Mobile Access Router Interface Configuration

This section describes how the mobile access router ports can be accessed through the CLI. The physical characteristics of the Cisco 3200 Series router interfaces are described in the “Cisco 3200 Series Router Hardware Reference.”

Fast Ethernet Interface Configuration

This section describes the basic configuration of the 10/100 Fast Ethernet interfaces. Depending on your requirements and the protocols you plan to route, you might also need to enter other configuration commands.

A Cisco device identifies a 10/100 Fast Ethernet interface by its slot number and port number, in the format slot/port. The slot/port address of a 10/100 Fast Ethernet interface on the MARC is 0/0.

The slot/port address of a 10/100 Fast Ethernet interface on the FESMIC depends upon the position of the rotary switch. For example, if the 4-port FESMIC rotary switch is in position 1, the ports are identified as 2/0, 2/1, 2/2, and 2/3. If the 2-port FESMIC rotary switch is in position 1, the ports are identified as 2/0 and 2/1. If the 4-port FESMIC rotary switch is in position 2, the ports are identified as 3/0, 3/1, 3/2, and 3/3. If the 2-port FESMIC rotary switch is in position 2, the ports are identified as 3/0 and 3/1.

To create a basic configuration, enable, and specify IP routing on a 10/100 Fast Ethernet interface, follow these steps:

	Command	Purpose
Step 1	Router> **enable** Password: password Router#	Enter enable mode. Enter the password. You have entered enable mode when the prompt changes to Router#.
Step 2	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter global configuration mode. You have entered global configuration mode when the prompt changes to Router(config)#.
Step 3	Router# **ip routing**	Enable routing protocols as required for your global configuration. This example uses IP routing.
Step 4	Router(config)# **interface FastEthernet** *0/0* Router(config-if)#	Enter interface configuration mode. You have entered interface configuration mode when the prompt changes to Router(config-if)#.
Step 5	Router(config-if)# **ip address** *ipaddress subnetmask*	Assign an IP address and subnet mask to the interface.
Step 6	Router(config-if)# **exit**	Exit back to global configuration mode.
Step 7	Router(config)# **Ctrl-z** Router#	When you finish configuring interfaces, return to enable mode.

Enabling the WMIC to FESMIC Connection

Unlike other Cisco 3200 Series router cards, the WMIC does not communicate with the mobile access router through the bus. It communicates through the Ethernet ports. Typically the WMIC Ethernet port is connected to a FESMIC Ethernet port. However, depending on the design, the WMIC Ethernet port might be connected to the MARC Ethernet port.

The following is an example of a configuration on the FESMIC that establishes connectivity between the WMIC and the FESMIC:

```
FESMIC#conf t
FESMIC#interface FastEthernet 2/1
FESMIC#no shut
```

The following is an example of a configuration on the WMIC that establishes connectivity between the WMIC and the FESMIC:

```
Wireless Mobile Interface Card (WMIC)#conf t
Wireless Mobile Interface Card (WMIC)#interface fastethernet 0/0
Wireless Mobile Interface Card (WMIC)#no shut
```

Serial Interface Configuration

You can configure the serial interfaces manually by entering Cisco IOS commands on the command line.

The slot/port address of a serial interface on the SMIC depends upon the position of the rotary switch. For example, if the 4-port SMIC rotary switch is in position 1, the ports are identified as 2/0, 2/1, 2/2, and 2/3. If the 2-port SMIC rotary switch is in position 1, the ports are identified as 2/0 and 2/1. If the 4-port SMIC rotary switch is in position 2, the ports are identified as 3/0, 3/1, 3/2, and 3/3. If the 2-port SMIC rotary switch is in position 2, the ports are identified as 3/0 and 3/1

Timesaver Before powering on the router, remove the serial cables from the serial ports. Otherwise when the router is powered on, if a serial cable is connected to one of the serial ports and the router does not have a valid configuration file stored in nonvolatile RAM (NVRAM), the router attempts to use the AutoInstall configuration feature to obtain a valid configuration by downloading a configuration file from the network. It can take several minutes for the process to time out.

	Command	Description
Step 1	Router> **enable** Password: *password* Router#	Enter privileged EXEC mode. Enter the password. You have entered enable mode when the prompt changes to Router#.
Step 2	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z.	Enter global configuration mode. You have entered global configuration mode when the prompt changes to Router(config)#.
Step 3	Router(config)# **ip routing**	Enable routing protocols as required for your global configuration. This example uses IP routing.
Step 4	Router(config)# **interface serial** *1/0* Router(config-if)#	Enter the interface configuration mode. You have entered interface configuration mode when the prompt changes to Router(config-if)#. For Cisco 3201 SMIC serial ports, slots 1, 2 and 3 are valid, and for each of these slots there are four serial ports: 0, 1, 2, and 3. For Cisco 3220 SMIC serial ports, slot 1 or 2 is valid. In the slot there are two serial ports: 0 and 1.
Step 5	Router(config-if)# **ip address** *ipaddress subnetmask*	Assign the IP address and subnet mask to the interface.
Step 6	Router(config-if)# **clockrate** *72000*	The router serial ports automatically detects the interface type (DTE or DCE) by the type of cable connected to the port. If you are using a port in DCE mode, connect a DCE cable and set the internal transmit clock signal (TXC) speed in bits per second. If you are using a port in DTE mode, the router automatically uses the external timing signal. You do not have to configure a clocking signal if the port is being used in DTE mode.

	Command	Description
Step 7	`Router(config-if)#` **`dce-terminal-timing-enable`**	If your serial port is DCE and the DTE side provides terminal timing (serial clock transmit external [SCTE] or terminal timing [TT]), you can use the **dce-terminal-timing-enable** command to configure the DCE to use the SCTE signal from the DTE. If the DTE side does not provide terminal timing then use the **no dce-terminal-timing-enable** command.
Step 8	`Router(config-if)#` **`exit`**	Exit to global configuration mode.

Step 9	`Router(config)# Ctrl-z`
	`Router#`
		Return to privileged EXEC mode.

AUX Interface Configuration for GPS Antenna

The following is an example configuration for configuring a Global Positioning System (GPS) receiver.

```
interface Serial1/0
 ip address 20.20.0.2 255.0.0.0
!
line aux 0
 modem InOut
 transport input all
 stopbits 1
 speed 4800
!
```

The following is home agent configuration that delivers GPS data to a PC connected to the **serial 1/0** interface.

```
ip host gps 2001 20.20.0.2
!
!
interface Serial1/0
 ip address 20.20.0.3 255.0.0.0
 clock rate 125000
!
interface Serial1/1
 physical-layer async
 no ip address
!
line 3
 no motd-banner
 no exec-banner
 exec-timeout 0 0
 no flush-at-activation
 no activation-character
 no vacant-message
 modem InOut
 autocommand  telnet gps /stream
 special-character-bits 8
 transport input all
 transport output telnet
 escape-character NONE
 autohangup
 speed 4800
 flowcontrol hardware
```

View GPS Data

To view the GPS data, you can use reverse Telnet from the router.

To simulate a GPS by using Hyperterminal, do the following:

Step 1 Set the connection parameters for the COM port connecting to the router to 4800/N/8/1.

Step 2 Select hardware flowcontrol. You can see NBMA data sent from GPS. For example:

```
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215737.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*32
$GPGLL,2728.2263,S,10302.8460,W,215737.641,V*2A
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPGSV,3,1,12,29,89,000,,05,69,000,,30,56,000,,09,53,000,*77
$GPGSV,3,2,12,26,37,000,,18,35,000,,21,30,000,,06,15,000,*76
$GPGSV,3,3,12,14,15,000,,23,10,000,,07,08,000,,24,-7,000,*68
$GPRMC,215737.641,V,2728.2263,S,10302.8460,W,,,110402,,*1B
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215738.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*3D
$GPGLL,2728.2263,S,10302.8460,W,215738.641,V*25
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215738.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*0A
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215739.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*3C
$GPGLL,2728.2263,S,10302.8460,W,215739.641,V*24
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215739.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*0B
$GPVTG,,T,,M,,N,,K*4E
$GPGGA,215740.641,2728.2263,S,10302.8460,W,0,00,50.0,0.0,M,,,,0000*32
$GPGLL,2728.2263,S,10302.8460,W,215740.641,V*2A
$GPGSA,A,1,,,,,,,,,,,,,50.0,50.0,50.0*05
$GPRMC,215740.641,V,2728.2263,S,10302.8460,W,0.00,,110402,,*05
$GPVTG,,T,,M,,N,,K*4E
```

Remote Access to the Router

The router can be accessed remotely by using applications such as Telnet. This section describes some of the remote access features.

Configure the Router to Accept a Remote Login

Use this procedure to configure the parameters that control remote access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

	Command	Purpose
Step 1	`Router(config)# line console 0`	Specifies the console terminal line.
Step 2	`Router(config-line)# exec-timeout 5`	Sets the interval that the EXEC command interpreter waits until user input is detected.
Step 3	`Router(config-line)# line vty 0 4`	Specifies a virtual terminal for remote console access

	Command	Purpose
Step 4	`Router(config-line)#password lineaccess`	Specifies a password on the line.
Step 5	`Router(config-line)#login`	Enables password checking at terminal session login.
Step 6	`Router(config-line)# end`	Exits configuration mode.

Configure the TTY Line

To configure the TTY line, do the following.

	Command	Purpose
Step 1	`Router(config)# line 1`	Enter line configuration mode.
Step 2	`Router(config-line)# modem inout`	Configure a line for both incoming and outgoing calls.
Step 3	`Router(config-line)# stopbits 1`	Set the number of stop bits.
Step 4	`Router(config-line)# speed 38400`	Set the baud rate.
Step 5	`Router(config-line)# transport input all`	Allow all protocols to be used when connecting to the line.
Step 6	`Router(config-line)# flowcontrol hardware`	Set the flow control.
Step 7	`Router(config-line)# exit`	Exit line configuration mode.

Access the Router with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start** > **Programs** > **Accessories** > **Telnet**.

If Telnet is not listed in your Accessories menu, select **Start** > **Run**, type **Telnet** in the entry 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 device IP address.

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

Step 4 At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Access the Router with Secure Shell

Secure Shell Protocol provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the home page of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/

Assign an IP Address to a Wireless Device by using the CLI

When you connect the wireless device to the wired LAN, the it links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the Ethernet and radio ports, the network uses the BVI.

Note The wireless device supports only one BVI. Configuring more than one BVI might cause errors in the 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 mask*	Assign an IP address and address mask to the BVI. **Note** If you are connected to the device using a Telnet session, you lose your connection to the device when you assign a new IP address to the BVI. If you need to continue configuring the device using Telnet, use the new IP address to open another Telnet session to the device.