Troubleshooting the Cisco 3200 Series Mobile Access Router

This document provides some information on troubleshooting a Cisco 3200 Series router. It includes the following:

- Wireless Card Default Configuration Recovery
- Disaster Recovery with TFTP Download
- Access ROM Monitor Mode
- Cisco IOS Image Download from the Console Port
- WMIC Image Update over FESMIC Port
- Flash and NVRAM File Management
- Mobile IP Debug
- Configuration Register Modification
- Password Recovery

Here are some important points to remember in troubleshooting Mobile IP clients:

- Mobile IP clients transmit type 10 ICMP Router Discovery Protocol packets to trigger the Mobile IP process. Routers respond with type 9 ICMP router advertisement packets. After this initial phase, the registration or deregistration process occurs.
- The hold time in the IRDP messages determines how fast the mobile node can detect movement between subnets. For example, the lifetime in the command **ip mobile host 10.0.150.200 interface FastEthernet0/0 lifetime 180** only makes the mobile node reregister with the home agent by using the current agent. It does not force it to switch agents (interfaces).
- The default hold time for IRDP is 30 minutes.

When the home agents or foreign agents advertise, they put a time limit (hold time) in the IRDP advertisements that tells the mobile node the interval the advertisements are valid. When a mobile node moves to a different subnet, the router waits until the hold time expires before it associates with a new interface (agent). If the lifetime on the registration expires before the hold time expires, the mobile node transmits a solicitation for the old agent (interface), until the hold time in the previous agent advertisement expires. If you do not adjust the IRDP timers, for 30 minutes the mobile node does not know that it has changed subnets.

Listed below are basic troubleshooting tips.

- Adjust the interval value for the foreign agent using the **ip irdp maxadvertinterval** *seconds* interface configuration command. Begin by setting the timer to 10 seconds and adjust as needed.
- Before you can ping a subnet on the mobile device, you must first define the subnet on the home agent.
- Redistribute mobile subnets on the home agent so that return traffic can be sent back to the mobile access router.
- Establish a return route from the foreign agent to the home agent.
- Avoid placing any routers behind the mobile device because it functions as a stub router.
- Ensure that the MD5 keys match between the mobile device and the home agent. Authentication is required.

Caveats and Error Messages

The following caveats and error messages apply to the Cisco 3200 Series Mobile Access Router.

Non-Cisco Components

Cisco does not provide:

- Power supply
- Cable assemblies
- Enclosure
- Stacking hardware
- Extractor tools
- Thermal solutions

Non-Cisco Cards

We recommend that you do not add non-Cisco cards that produce peripheral component interconnect (PCI) bus signals. Adding non-Cisco cards that generate PCI bus signals can produce unpredictable results. (Cisco cards do not use ISA bus signals, but all the cards will pass the ISA signals through the bus.)

Cisco MIC Mismatch Error

Most of the Mobile Access Router Card (MARC) stacks are fixed configuration and the stack cannot be modified. The router generates the following error message if the cards are stacked in the router improperly or a MIC in the stack is not supported by the companion MARC.

The following error message is displayed:

```
**************************************************************************
 *            ****NON RECOVERABLE ERROR OCCURRED ****                     *
 *                                                                        *
 *   1) The three cards (3220MARC, 3220SMIC and 3220FESMIC) must be       *
 *      plugged in for the 3220 Mobile Router to be operational.          *
 *                                                                        *
 *   2) The following cards are unsupported                               *
 *      card in slot 1 is 3201SMIC                                       *
 *      card in slot 2 is an unknown card                               *
 *                                                                        *
 *   3) Please power down the router and remove any unsupported cards     *
 *      plugged into the 3220MARC.                                        *
 *                                                                        *
 *   For more information, please refer to the user documentation         *
 *                                                                        *
 **************************************************************************
```

After displaying the error message, the router goes into ROMMON mode. You must modify the card stack before the router will boot by using the Cisco IOS.

Rotary Switch Position Error

The router generates the following error message if the rotary switch is set in a position that is unsupported.

```
**************************************************************************
 *          ****ROTARY SWITCH CONFIGURATION ERROR****                     *
 *                                                                        *
 *   One of the MICs has the rotary switch wrongly configured at          *
 *   position 3. Please change rotary switch configuration on this MIC    *
 *   to a valid position as described below.                              *
 *                                                                        *
 *   Both the MICs with switch positions at 2 and 3 are disabled.         *
 *    Instructions:                                                       *
 *      1) Only switch positions 0-2 are supported.                       *
 *      2) Selecting the same switch position on multiple MICs is not     *
 *         supported.                                                     *
 *      3) To change switch configuration please power down router.       *
 *                                                                        *
 *   For more information, please refer to the hardware documentation.    *
 *                                                                        *
 **************************************************************************
```

After displaying the error message, the router goes into ROMMON mode. You must modify the rotary switch before the router will boot by using the Cisco IOS.

Wireless Card Default Configuration Recovery

It is possible that you might be locked out of the Wireless Mobile Interface Card (WMIC) as the result of an error in an access list or typo in a password. These parameters are stored in the config.txt file in Flash memory.

Caution This procedure erases the wireless card configuration. If you delete the configuration and do not have a copy, you will have to create the configuration from scratch.

To recover control of the router, connect a terminal to the console port of the WMIC and do the following:

Step 1 Enter the **reload** command.

```
c3201br#reload
```

Step 2 Press the Escape (ESC) key twice when the boot process begins to display a bootloader prompt.

```
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!
ethernet link up, 100 mbps, full-duplex
Ethernet port 0 initialized: link is up
Loading
"flash:/c3201-k9w7-mx.122/c3201-k9w7-mx.122"...##########################################
#####################################################################bad
mzip file, unknown zip method

Error loading "flash:/c3201-k9w7-mx.122/c3201-k9w7-mx.122"

Interrupt within 5 seconds to abort boot process.
Boot process terminated.

The system is unable to boot automatically. The BOOT
environment variable needs to be set to a bootable
image.

C3201 Boot Loader (C3201-BOOT-M), Version 12.2 [hftseng-c3201wmic 102]
compiled Sun 29-Feb-04 15:59 by hftseng

bridge:
```

Step 3 Enter the **dir flash:** command to verify the config.txt file is in memory.

```
bridge: dir flash:
Directory of flash:/
```

```
2    -rwx  4114432   <date>              c3201-k9w7-tar
3    -rwx  180       <date>              env_vars
4    -rwx  1091      <date>              config.txt
5    drwx  384       <date>              c3201-k9w7-mx.122
142  -rwx  1091      <date>              config.txt.saved
143  -rwx  5         <date>              private-config

7828992 bytes available (8169984 bytes used)
```

Step 4 Enter the **delete flash:config.txt** command.

```
bridge: delete flash:config.txt
Are you sure you want to delete "flash:config.txt" (y/n)?y
File "flash:config.txt" deleted

bridge:
```

Step 5 Reboot the router.

Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the command–line interface (CLI). However, if the router is unable to boot the Cisco IOS software, you can load new software while in ROM monitor mode.

This section describes how to load a Cisco IOS software image from a remote TFTP server to the router Flash memory.

The following steps should be performed while in ROM monitor mode.

Step 1 Use the appropriate commands to enter all the required variables and any optional variables described earlier in this section.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld -r
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to Flash memory. You can then use the image that is in Flash memory the next time you enter the **reload** command.

You will see output similar to the following:

```
rommon 4 > tftpdnld

          IP_ADDRESS: 1.6.88.21
       IP_SUBNET_MASK: 255.255.0.0
      DEFAULT_GATEWAY: 1.6.0.1
          TFTP_SERVER: 223.255.254.251
            TFTP_FILE: cisco/c3200-i11k9-mz.bin
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter y in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router begins to download the new file.

Entering Ctrl-C or Break stops the transfer before the Flash memory is erased.

TFTP Download Command Variables

This section describes the system variables that can be set in ROM monitor mode and that are used during the TFTP download process.

Note The commands described in this section are case-sensitive and must be entered exactly as shown in the tables.

Required Variables

These variables must be set with these commands before using the **tftpdnld** command:

Command	Description
IP_ADDRESS= *ip_address*	IP address of the router.
IP_SUBNET_MASK= *ip_address*	Subnet mask of the router.
DEFAULT_GATEWAY= *ip_address*	IP address of the default gateway of the router.
TFTP_SERVER= *ip_address*	IP address of the TFTP server from which the software will be downloaded.
TFTP_FILE= *filename*	The name of the file that will be downloaded to the router.

Optional Variables

These variables can be set with these commands before using the **tftpdnld** command:

Variable	Command
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process; for example: `Initializing interface.` `Interface link state up.` `ARPing for 1.4.0.1` `ARP reply for 1.4.0.1 received.  MAC address 00:00:0c:07:ac:01`	**TFTP_VERBOSE=** *setting*

Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Amount of time, in seconds, before the download process times out. The default is 2, 400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Access ROM Monitor Mode

The ROM monitor firmware runs when the router is powered up or reset and helps to initialize the processor hardware and boot the operating system software. If there is no Cisco IOS software image loaded on the router, ROM monitor is the default operating system. If there is an Cisco IOS software image, you can still force the router to boot to the ROM monitor by pressing the break key within the first 60 seconds of the router booting or changing the configuration register so the router looks for the ROM monitor bootable image first. In ROM monitor mode, you can perform certain configuration tasks, such as to boot without loading the configuration file to recover a lost password or to download Cisco IOS software over the console port.

To use the ROM monitor, you must be using a terminal or PC that is connected to the router over the console port.

Timesaver Break (system interrupt) is always enabled for 60 seconds after the router reboots, regardless of whether it is set to on or off in the configuration register. During this 60-second window, you can break to the ROM monitor prompt by pressing the Break key.

Take these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted:

	Command	Purpose
Step 1	`Router>`**enable**	Enters privileged mode. If there is an enable password configured, enter the enable password to enter privileged EXEC mode.
Step 2	`Router#`**show version**	Displays the current register setting. Record the configuration register setting, which is typically 0x2102, so the register can be changed back to the original setting.
Step 3	`Router#`**configure terminal**	Enters global configuration mode.
Step 4	`Router(config)#`**config-reg 0x0**	Resets the configuration register.
Step 5	`Router(config)#`**exit**	Exits global configuration mode.

	Command	Purpose
Step 6	`Router#`**reload**	Reboots the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. Refer to the **boot** command in the "ROM Debug Commands" section.
	After the router reboots, it is in ROM monitor mode. To return the router to its original state, repeat the process, substituting the original value for the register.	

ROM Monitor Commands

Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 2>?
alias              set and display aliases command
boot               boot up an external process
break              set/show/clear the breakpoint
confreg            configuration register utility
cont               continue executing a downloaded image
context            display the context of a loaded image
cookie             display contents of cookie PROM in hex
copy               Copy a file-copy [-b <buffer_size>] <src_file>
<dst_file>
delete             Delete file(s)-delete <filenames ...>
dir                List files in directories-dir <directory>
dis                display instruction stream
dnld               serial download a program module
format             Format a filesystem-format <filesystem>
frame              print out a selected stack frame
fsck               Check filesystem consistency-fsck <filesystem>
help               monitor builtin command help
history            monitor command history
meminfo            main memory information
mkdir              Create dir(s)-mkdir <dirnames ...>
more               Concatenate (type) file(s)-cat <filenames ...>
rename             Rename a file-rename <old_name> <new_name>
repeat             repeat a monitor command
reset              system reset
rmdir              Remove a directory
set                display the monitor variables
stack              produce a stack trace
sync               write monitor environment to NVRAM
sysret             print out info from last system return
tftpdnld           tftp image download
unalias            unset an alias
unset              unset a monitor variable
xmodem             x/ymodem image download
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, refer to the documentation for that product for information on how to send a Break command.

ROM Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or is halted. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

```
"xxx: kernel context state is invalid, can not proceed."
```

The following are ROM monitor debugging commands:

- **stack** or **k**—produce a stack trace; for example:

```
rommon 2> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**—displays processor context; for example:

```
rommon 2> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**—displays an individual stack frame.
- **sysret**—displays return information from the last booted system image. This information includes the reason for terminating the image, a stack dump of up to eight frames, and, if an exception is involved, the address where the exception occurred; for example:

```
rommon 3 > sysret
System Return Info:
count: 19,  reason: reset
pc:0x0,  error address: 0x0
Stack Trace:
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
rommon 4 >
```

- **meminfo**—displays size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of nonvolatile RAM (NVRAM); for example:

```
rommon 1> meminfo
Main memory size: 128 MB.
Available main memory starts at 0x1b000, size 130964KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 128KB
rommon 2 >
```

ROM Monitor Image Download by using TFTP

This section contains procedures for downloading software in ROM Monitor (ROMMON) mode by using the **tftpdnld** command.

Complete these steps to upgrade the ROMMON image from ROMMON mode.

Step 1 Download the ROMMON image from CCO, and place it on your Trivial File Transfer Protocol (TFTP) server.

Step 2 Place the router in ROMMON mode by sending a telnet **break** command during the router reboot sequence. The following prompt will be displayed, indicating entry into ROMMON mode:

```
rommon >
```

Step 3 In ROMMON mode, set the following parameters by typing the names followed by an equals sign as shown, and then typing a value for the parameter.

Table 18-1 describes the type of value to provide for each parameter.

Table 18-1 ROMMON Parameters and Values

Parameter	Value
IP_ADDRESS=	IP address of the router
IP_SUBNET_MASK=	Subnet mask of the router
DEFAULT_GATEWAY=	IP address of the router's default gateway
TFTP_SERVER=	IP address of the TFTP server on which the ROMMON image is located
TFTP_FILE=	The path and filename of the ROMMON image

Step 4 Verify the parameter settings by entering the **set** command. Correct any mistakes by reentering the parameter and value.

```
rommon> set
TFTP_CHECKSUM=0
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=1.6.0.1
TFTP_SERVER=223.255.254.254
IP_ADDRESS=1.6.97.20
TFTP_FILE=C3200_RM_ALT.srec.122-1r.XE2
```

Step 5 Upgrade the ROMMON image by entering the **tftpdnld -u** command. Sample output is shown below.

```
rommon >tftpdnld -u
IP_ADDRESS: 1.6.97.20
```

```
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 1.6.0.1
TFTP_SERVER: 223.255.254.254
TFTP_FILE: C3200_RM_ALT.srec.122-1r.XE2
WARNING: alternate copy of rommon exists, filename: C3200_RM_ALT.srec all existing data in
the alternate copy of rommon will be lost.
 Do you wish to continue? y/n:  [n]:
```

Step 6 Enter **y** to start the download. A series of exclamation points (!!!!!!) indicates that the image is downloading successfully. The router will reboot when the download is complete.

Note You may need to reset the router while in ROMMON mode by entering the **reset** command before entering the **tftpdnld** command. The router will prompt you to do this if needed. If prompted to reset the router, you must reset the router and then follow Step 2 through Step 6 to update the ROMMON image.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are only displayed on the console when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Cisco IOS Image Download from the Console Port

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. After download, the file is saved to the Flash memory.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the **ROM monitor** command.

Xmodem is used in disaster recovery situations where the router has no valid Cisco IOS software or bootflash image to boot from and hence, only boots up in ROMmon. This procedure can also be used where there are no Trivial File Transfer Protocol (TFTP) servers or network connections, and a direct PC connection (or through a modem connection) to the router's console is the only viable option. Because this procedure relies on the console speed of the router and the serial port of the PC, it can take a long time to download an image.

Configure Windows HyperTerminal for 8-N-1 at 9600 bps and connect your PC's serial port to the console port of the router. Once connected, you need to get into the ROMmon prompt (rommon 1>). Typically, if the Cisco IOS software image and bootflash image are both corrupt, the router only comes up in ROMmon mode. If the former is not true and you need to get into the ROMmon prompt, change the configuration register (typically 0x2102 as given by show version) to 0x0 as described in the "Access ROM Monitor Mode" section.

Console port PC settings are also described in the "Terminal Configuration" section of the "Cisco 3200 Series Mobile Access Router Interfaces" chapter.

Follow the steps below to run Xmodem:

Step 1 Move the image file to the local drive where the Xmodem will execute.

Step 2 Launch the terminal emulation application, such as HyperTerminal.

Note You might have to reset the registry so the router boots from rommon.

Step 3 Enter the **xmodem** command.

Following is the syntax and descriptions for the **xmodem** console download command. For example:

```
rommon 1 >xmodem c3220-i11k9-mz.123-2.XA2.bin
```

The router displays the message:

```
Do you wish to continue? y/n  [n]:  y
```

Step 4 Type **y** and press **Enter**. The system displays a message indicating that it is ready to receive the file:

```
Ready to receive file c3220-i11k9-mz.123-2.XA2.bin
```

Step 5 Click **Transfer**>**Send File**. The **Send File** window displays.

Step 6 Type the file name in the **Filename** field or use the **Browse** button to select the file from the Explorer.

Step 7 Select the protocol, typically Xmodem, from the **Protocol** drop-down list.

Step 8 Click **Send**. The **Xmodem** file send window displays. Note that it might take a few seconds before the file transfer begins.

Download Errors

The following error displays if you are try to download a corrupt file, a file that is not an executable file, or a file that is not acceptable to the router. For example, if you try to download a Cisco 3250 base IOS image to a Cisco 3200 Series router.

```
Ready to receive file c3200-i11-mz.122-15.ZL.bin
BB0Download Complete!

ERR:File not a valid executable
rommon 36 >
```

xmodem Syntax

The syntax for the **xmodem** command is as follows:

```
xmodem [-ucyrx] destination_file_name
```

u	(Optional) Performs and upgrade of the ROMMON. System reboots after the file is upgraded.
c	(Optional) Performs the download using 16-bit cyclic redundancy check (CRC-16) error checking to validate packets. Default is 8-bit CRC.
y	(Optional) Sets the router to perform the download using Ymodem protocol. Default is Xmodem protocol. The protocols differ as follows: • Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size. • Ymodem uses (CRC)-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.
r	(Optional) Image is loaded into DRAM for execution. Default is to load the image into Flash memory.
x	(Optional) Image is loaded into DRAM without being executed.
destination_file_name	The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

WMIC Image Update over FESMIC Port

This section describes the procedure for updating the software image on a MARC and WMIC over wired connection to a TFTP server through a port on FESMIC. It is also possible to update the software image on the WMIC by using a wireless connection; however, it is not described here.

To download the image, do the following:

Step 1 Add following to the configuration on the MARC. The IP addresses used are for illustration only and should be replaced by the IP addresses used in your configuration.

```
ip dhcp pool fa0
   network 10.0.0.0 255.0.0.0 (network <network addr of Fa0>)
   default-router 10.0.0.1 (default-router <ip addr of fa0/0)
ip dhcp pool vlan1
   network 30.0.0.0 255.0.0.0 (network <network addr of Vlan1>)
   default-router 30.0.0.1 (default-router <ip addr ofVlan1)
no spanning-tree vlan 1
no spanning-tree vlan 2
interface FastEthernet0/0
 ip address 10.0.0.1 255.0.0.0 (ip address <ip addr>)
 ip nat inside
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
interface FastEthernet1/1
 switchport access vlan 2
 no ip address
interface Vlan1
 ip address 30.0.0.1 255.0.0.0 (ip address <ip addr>)
 ip nat inside
interface Vlan2
 ip address 1.7.43.9 255.255.0.0  (ip address <ip addr of TFTP network>)
 ip nat outside
```

```
ip nat inside source list 100 interface Vlan2 overload
ip route 223.255.254.0 255.255.255.0 Vlan2 (ip route <TFTP server network> Vlan2)
access-list 100 permit ip any any
```

Procedure:

Step 2 Use default configuration on Cisco 3201 WMIC. By default, the Cisco 3201 WMIC uses DHCP to acquire an IP address for Bridge Group Virtual Interface (BVI). The Cisco 3201 WMIC Workgroup Bridge BVI IP address is 10.0.0.2 and Cisco 3201 WMIC Root Bridge BVI IP address is 30.0.0.2. These are the Telnet addresses.

Step 3 Log-in into the Cisco 3251 through its console port and download image.

Step 4 Telnet into the WMIC after log-in into the MARC through its console port and then download image.

Flash and NVRAM File Management

The router uses a random access file system. It is not necessary to erase an entire file space to reclaim memory held by deleted files, because the random access file system has a hierarchical directory structure that allows you to delete individual files. When the file is deleted, the memory space is freed. In contrast, the low end system (LES) file system used by other platforms, such Cisco 2500 Series routers and Cisco 5200 Series routers, has no provision for reclaiming the space from deleted files.

NVRAM is the segment of Flash memory reserved exclusively by Cisco IOS to store the configuration files for the router. When an Cisco IOS image is loaded, it reads the configuration files to determine which interfaces to bring up and what kind of configurations to use.

Delete Configuration Files

To erase a configuration file, use the **delete nvram:config** command:

```
Router#delete nvram:config
Delete filename [config]? filename
Delete nvram:config? [confirm] filename
Router#
```

or if the file is in Flash (the device name is optional)

```
Router#delete startup-config
Delete filename [startup-config]? filename
Delete flash:startup-config? [confirm] filename
Router#
```

Erase the Flash File System

To delete all files in Flash, use the **erase flash:** command:

```
Router#erase flash:
Erasing the flash filesystem will remove all files! Continue? [confirm]
flashfs[10]: 0 files, 1 directories
flashfs[10]: 0 orphaned files, 0 orphaned directories
flashfs[10]: Total bytes: 31739904
flashfs[10]: Bytes used: 4096
flashfs[10]: Bytes available: 31735808
flashfs[10]: flashfs fsck took 5 seconds.
Erase of flash: complete
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
copy	Duplicates a file.
delete	Deletes a file.

Command	Description
dir	Displays a list of files.
more	Continues a list that has been paused.
rename	Changes the name of a file.
verify	Verifies the checksum of a file before using it.
cd	Changes the default directory or file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.
format	Formats a file system.
fsck	Validates a file system.
rmdir	Removes a directory.

Mobile IP Debug

This section shows normal operating debugs and configurations of Mobile IP.

Note TLV stands for Type, Length, Value. It is the template used in registration request and reply messages. See RFC 2002 for more information.

Debug Commands for Troubleshooting

The following debug commands are useful in troubleshooting Mobile IP clients:

- debug arp
- debug ip icmp
- debug ipmobile host
- debug ip mobile
- debug ip packet detail

The **debug arp** command shows you the mobile node ARPs on the local subnet. It can also help determine if the mobile node is causing a **MobileIP: FastEthernet1/0 add 10.0.150.200 rejected** error message or if the interface does not have IRDP configured.

The **debug ip icmp** command shows you the mobile node solicitations and the replies. The **debug ip mobile advertisements** command only shows you the foreign agent replies to solicitations from the Mobile IP client or unsolicited advertisements, not the actual Mobile IP client solicitations.

The **debug ip mobile** command is a combination of the **debug ip mobile host** and **debug ip mobile advertisements** commands. The **debug ip mobile host** command shows all of the normal Mobile IP debugs except for the IRDP replies to solicitations and the skip2TLV messages as the home agent or foreign agent searches the request or the reply for information.

The **debug ip packet detail** command is used with an access list and shows you all the Mobile IP packets at the foreign agent since they are all still process switched.

Good Registration from a Mobile Client on a Foreign Network

These debug results show what occurs during a normal *good* registration. In these examples:

- The Mobile IP client is coming up from a power on state.
- The mobile node ARPs in the beginning against the RFC and the router rejects the IP address.
- The Mobile IP client registration request is rejected the first time it tries to register with the home agent because its clock is too far out of synchronization with the home agent clock.

The home agent registration reply contains the offset the Mobile IP client will use for the next registration request. The mobile node registers successfully on the second attempt, after adjusting its timestamp with the offset sent by the home agent.

On the Foreign Agent:

```
*Mar 16 22:09:15:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27773,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:15: Care-of address: 192.1.1.1
*Mar 16 22:09:15: ICMP: src=192.1.1.1, dst=255.255.255.255, irdp advertisement sent
*Mar 16 22:09:15: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:15: IRDP: address=192.1.1.1 preference=0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:18: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:19: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
*Mar 16 22:09:20: IP ARP req filtered src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
0000.0000.0000 wrong cable, interface FastEthernet1/0
*Mar 16 22:09:20: ICMP: rdp solicit rcvd type 10, code 0, from 10.0.150.200
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:20: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
*Mar 16 22:09:20:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27774,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:20: Care-of address: 192.1.1.1
*Mar 16 22:09:20: ICMP: src=192.1.1.1, dst=10.0.150.200, irdp advertisement sent
*Mar 16 22:09:20: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:20: IRDP: address=192.1.1.1 preference=0
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:20: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received registration id mismatch (133) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.150.200 accepted
*Mar 16 22:09:21: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
```

```
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received accept (0) reply for MN 10.0.150.200 on FastEthernet0/0 using HA
10.0.150.6 lifetime 180
MobileIP: Reply in for MN 10.0.150.200, accepted
MobileIP: Update visitor table for MN 10.0.150.200
MobileIP: Tunnel0 (IP/IP) created with src 192.1.1.1 dst 10.0.150.6
MobileIP: ARP entry for MN 10.0.150.200 inserted
MobileIP: Visitor timer started for MN 10.0.150.200, lifetime 180
MobileIP: FA dequeued MN 10.0.150.200 from register table
MobileIP: MN 10.0.150.200 visiting on FastEthernet1/0
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: swif coming up Tunnel0
```

Advertisements are sent out.

```
*Mar 16 22:09:24:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27773,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 22:09:24: Care-of address: 192.1.1.1
*Mar 16 22:09:24: ICMP: src=192.1.1.1, dst=255.255.255.255, irdp advertisement sent
*Mar 16 22:09:24: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 22:09:24: IRDP: address=192.1.1.1 preference=0
```

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Identification field has timestamp 240175185 secs greater than our current time
03/16/93 03:48:14 (> allowed 255 secs) for MN 10.0.150.200
*Mar 15 19:48:14: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode registration id mismatch (133), reason Bad identifier (3)
MobileIP: HA rejects registration for MN 10.0.150.200 - registration id mismatch (133)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 requested broadcast support, but disabled locally
MobileIP: Mobility binding for MN 10.0.150.200 created
MobileIP: Tunnel0 (IP/IP) created with src 10.0.150.6 dst 192.1.1.1
MobileIP: Roam timer started for MN 10.0.150.200, lifetime 180
MobileIP: MN 10.0.150.200 is now roaming
MobileIP: Insert host route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: HA accepts registration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
MobileIP: swif coming up Tunnel0
```

Deregistration When a Mobile Node Returns to the Home Network

This example shows the mobile node deregistration when it arrives on its home network. The IKV mobile client repeats the deregistration process 3 times.

On the Home Agent:

```
*Mar  1 03:31:51: IP: s=10.0.150.200 (FastEthernet0/0), d=255.255.255.255, len 28, rcvd 0
*Mar  1 03:31:51:     ICMP type=10, code=0
*Mar  1 03:31:54:
MobileIP: Agent advertisement sent out FastEthernet0/0: type=16, len=6, seq=0,
lifetime=36000, flags=0x2400(rbHfmGv-rsv-),
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=255.255.255.255 (FastEthernet0/0), len 44,
sending broad/multicast
*Mar  1 03:31:54:     ICMP type=9, code=0
*Mar  1 03:31:54: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:31:54:     UDP src=1050, dst=434
MobileIP: HA 92 received deregistration for MN 10.0.150.200 on FastEthernet0/0 using COA
10.0.150.200 HA 10.0.150.6 lifetime 0 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: HA accepts deregistration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200, len 70, cef process switched
*Mar  1 03:31:54:     UDP src=434, dst=1050
*Mar  1 03:31:54: IP ARP: creating incomplete entry for IP address: 10.0.150.200 interface
FastEthernet0/0
*Mar  1 03:31:54: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.200 0000.0000.0000 FastEthernet0/0
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
sending
*Mar  1 03:31:54:     UDP src=434, dst=1050
*Mar  1 03:31:54: IP ARP throttled out the ARP Request for 10.0.150.200
*Mar  1 03:31:54: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
encapsulation failed
*Mar  1 03:31:54:     UDP src=434, dst=1050
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.200
*Mar  1 03:31:54: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
*Mar  1 03:32:01: IP: s=10.0.150.200 (FastEthernet0/0), d=255.255.255.255, len 28, rcvd 0
*Mar  1 03:32:01:     ICMP type=10, code=0
*Mar  1 03:32:01: IP ARP: Gleaning entry for 10.0.150.200, 0010.a403.1357
```

Transition from the Home Network to a Foreign Network

This debug example shows the mobile node transitioning from the home network to a foreign network. For the mobile node to send a registration request, it must first be alerted that it has changed subnets. It does this by waiting for the advertisement timeout to expire, and then sending a solicitation.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 requested broadcast support, but disabled locally
MobileIP: Mobility binding for MN 10.0.150.200 created
```

```
MobileIP: Tunnel0 (IP/IP) created with src 10.0.150.6 dst 192.1.1.1
MobileIP: Roam timer started for MN 10.0.150.200, lifetime 180
MobileIP: MN 10.0.150.200 is now roaming
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent rep src 10.0.150.200 0002.4bb0.ecb0,
                 dst 10.0.150.200 0002.4bb0.ecb0 FastEthernet0/0
MobileIP: Gratuitous ARPs sent for MN 10.0.150.200 MAC 0002.4bb0.ecb0
MobileIP: Insert host route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: HA accepts registration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:52:31: IP ARP: creating incomplete entry for IP address: 10.0.150.5 interface
FastEthernet0/0
*Mar  1 03:52:31: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.5 0000.0000.0000 FastEthernet0/0
*Mar  1 03:52:31: IP ARP throttled out the ARP Request for 10.0.150.5
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
*Mar  1 03:52:31: IP ARP: rcvd rep src 10.0.150.5 0010.7bb2.8d80, dst 10.0.150.6
FastEthernet0/0
MobileIP: swif coming up Tunnel0
```

Transition from a Foreign Network to the Home Network

This debug example shows the mobile node transitioning from a foreign network to a home network.

On the Home Agent:

```
*Mar  1 03:56:35: IP: s=10.0.150.6 (local), d=255.255.255.255 (FastEthernet0/0), len 44,
sending broad/multicast
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:56:35:     UDP src=1050, dst=434
MobileIP: HA 92 received deregistration for MN 10.0.150.200 on FastEthernet0/0 using COA
10.0.150.200 HA 10.0.150.6 lifetime 0 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36F6C end FA36F82
MobileIP: Skip2TLV look for type 32, addr start FA36F82 end FA36F82
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Delete tunnel route for 10.0.150.200 via gateway 192.1.1.1
MobileIP: Deleted Tunnel0 src 10.0.150.6 dest 192.1.1.1
*Mar  1 03:56:35: ip_mobile_query
MobileIP: HA route maint started with index 0
MobileIP: MN 10.0.150.200 back home
*Mar  1 03:56:35: IP ARP: creating incomplete entry for IP address: 10.0.150.200 interface
FastEthernet0/0
*Mar  1 03:56:35: IP ARP: sent req src 10.0.150.6 0002.4bb0.ecb0,
                 dst 10.0.150.200 0000.0000.0000 FastEthernet0/0
*Mar  1 03:56:35: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
MobileIP: Get ARP entry for MN 10.0.150.200 succeeded
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.200 0010.a403.1357,
                 dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
MobileIP: Gratuitous ARPs sent for MN 10.0.150.200 MAC 0010.a403.1357
MobileIP: HA accepts deregistration from MN 10.0.150.200
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
*Mar  1 03:56:36: IP: s=10.0.150.6 (local), d=10.0.150.200, len 70, cef process switched
```

```
*Mar  1 03:56:36:     UDP src=434, dst=1050
*Mar  1 03:56:36: IP: s=10.0.150.6 (local), d=10.0.150.200 (FastEthernet0/0), len 70,
sending
*Mar  1 03:56:36:     UDP src=434, dst=1050
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.200
*Mar  1 03:56:36: IP ARP: rcvd req src 10.0.150.200 0010.a403.1357, dst 0.0.0.0
FastEthernet0/0
*Mar  1 03:56:36: IP ARP: rcvd req src 10.0.150.200 0010.a403.1357, dst 10.0.150.6
FastEthernet0/0
*Mar  1 03:56:36: IP ARP: sent rep src 10.0.150.6 0002.4bb0.ecb0,
                dst 10.0.150.200 0010.a403.1357 FastEthernet0/0
*Mar  1 03:56:36: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
FastEthernet0/0
```

Verifying Operation

Verify that the foreign agent is sending agent advertisements.

Turn on **debug ip mobile advertise** on the foreign agent. The following messages should be displayed periodically (based on *number* in the **ip irdp max** command).

```
00:08:11: MobileIP: Agent advertisement sent out Ethernet3/1: type=16, len=10, seq=3,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
00:08:11: Care-of address: 27.0.0.12
```

If not, make sure configuration for interface and care-of address is correct.

Verify the mobile access router receives agent advertisements.

Turn on **debug ip icmp** on mobile access router. The following message should be displayed periodically.

```
2w2d: ICMP: rdp advert rcvd type 9, code 0, from 27.0.0.12
```

Make sure interface receiving agent advertisement is configured for roaming. Enter the **show ip mobile router interface** command to display interface information.

Verify the mobile access router learns about the foreign agent.

Enter the **show ip mobile router agent** command on the mobile access router to display foreign agent information.

Verify mobile access router registration.

Turn on **debug ip mobile router** on the mobile access router. The following messages should be displayed.

```
MobileRouter: New FA 27.0.0.12 coa 27.0.0.12 int Ethernet0/1 MAC 0050.50c1.c855
2w2d: MobileRouter: Register reason: isolated
2w2d: MobileRouter: Snd reg request agent 27.0.0.12 coa 27.0.0.12 home 9.0.0.1 ha 29.0.0.4
lifetime 36000 int Ethernet0/1 flag sbdmgvt cnt 0 id B496B69C.55E77974
2w2d: MobileRouter: Status Isolated -> Pending
```

Enter the **show ip mobile router registration** command on mobile access router to display registration information. When mobile access router is registered, the **show ip mobile router registration** command displays when request was last accepted and the **show ip mobile router** command displays the status of the register.

If the mobile access router is not registered, turn on **debug ip mobile host** on the home agent to see registration debugging messages. Make sure the SPI and key are same on both the mobile access router and the home agent by using the **show ip mobile secure home-agent** and **show ip mobile secure host** commands. Make sure the home agent knows how to reach foreign agent by using the **show ip route** command, which displays the route to the care-of address.

Turn on **debug ip mobile host** on both the foreign agent and the home agent to see Mobile IP activities.

Enter the **show ip mobile router** command to display mobile access router information.

Turn on **debug tunnel** on the home agent, the foreign agent, and the mobile access router. For packets that are process switched, the following messages are displayed.

```
00:55:33: Tunnel0: to decaps IP/IP packet 29.0.0.4->27.0.0.12 (len=140, ttl=254)
00:55:33: Tunnel0: decapsulated IP/IP packet 29.0.0.4->9.0.0.1 (len=120 ttl=255)
```

For packets that are fast switched, use the **show ip cache** command to display the cache entries.

Error Codes

This section provides a summary of error codes returned in registration replies from the home agent. Some configuration errors on the home agent do not return a registration reply and so no code is sent to the foreign agent or mobile node. One of these types of errors occurs when the mobile node does not have a security association (SA). In this case, the home agent registers an error and drops the packet. The best place to debug general problems is on the home agent.

Error Code	Description
131	Security Association mismatch, such as bad password, bad security parameter index (SPI)
133	Time clocks not synchronized (mismatched id)
128	Configuration error on HA

Foreign Agent Registration Error Codes

Code	Description
64	* reason unspecified *
65	* administratively prohibited *
66	* insufficient resource *
67	* MN failed authentication *
68	* HA failed authentication *
69	* requested lifetime too long *
70	* poorly formed request *
71	* poorly formed reply *
72	* requested encapsulation unavailable *
73	* requested Van Jacobson compression unavailable *
74	* reverse tunnel unsupported *

75	* reverse tunnel mode only *
80	* unreachable base value *
80	* home network unreachable *
81	* HA host unreachable (not used, but in RFC2002)*
82	* HA port unreachable (not used, but in RFC2002)*
83	* HA unreachable (not used, but in RFC2002)*

Home Agent Registration Error Codes

Code	Description
128	* reason unspecified *
129	* administrative prohibited *
130	* insufficient resource *
131	* MN failed authentication *
132	* FA failed authentication *
133	* registration identification mismatched *
134	* poorly formed request *
135	* too many simultaneous bindings *
136	* unknown HA address *
137	* reverse tunnel unavailable *
138	* reverse tunnel mode only *
139	* unsupported encapsulation *
140	* active HA failed authentication (not in RFC2002)*

Debug Troubleshooting Scenarios

This section describes the following specific problems:

- Bad Password
- Bad SPI
- No IRDP on Foreign Agent Interface
- No IRDP on Home Agent Interface
- Time Clocks Not Synchronized on Mobile Node and Home Agent (usually not a problem)
- Missing ip mobile virtual-network Command on the Home Agent
- Mobile Node Is Not On Line
- No Security Association for the Mobile Node on the Home Agent (a home agent configuration error)

Bad Password

The debug messages in this example show what happens on the home agent and foreign agent when either the home agent or the Mobile IP client is configured with an incorrect password. The passwords on the home agent and Mobile IP client must match.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - invalid authenticator for MN 10.0.150.200
*Mar  1 03:10:32: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode MN failed authentication (131), reason Bad authenticator (2)
MobileIP: HA rejects registration for MN 10.0.150.200 - MN failed authentication (131)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3D04EAC end 3D04EC2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
MobileIP: FA received MN failed authentication (131) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3D04EA8 end 3D04EBE
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
```

Bad SPI

This debug example shows when the SPI specified on the home agent does not match the SPI specified on the Mobile IP client.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36BAC end FA36BC2
MobileIP: Skip2TLV look for type 32, addr start FA36BC2 end FA36BC2
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - SPI 100 for MN 10.0.150.200 is not configured
*Mar  1 03:05:08: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode MN failed authentication (131), reason Bad SPI (4)
MobileIP: HA rejects registration for MN 10.0.150.200 - MN failed authentication (131)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 101) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
*Mar  2 05:25:19: IP: s=10.0.150.200 (FastEthernet1/0), d=192.1.1.1 (FastEthernet1/0), len
74, rcvd 3
*Mar  2 05:25:19:     UDP src=1050, dst=434
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B01A0C end 3B01A22
*Mar  2 05:25:19: IP: s=10.0.150.5 (local), d=10.0.150.6, len 74, cef process switched
*Mar  2 05:25:19:     UDP src=434, dst=434
*Mar  2 05:25:19: IP: s=10.0.150.5 (local), d=10.0.150.6 (FastEthernet0/0), len 74,
sending
*Mar  2 05:25:19:     UDP src=434, dst=434
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.0.150.6
*Mar  2 05:25:19: IP: s=10.0.150.6 (FastEthernet0/0), d=10.0.150.5 (FastEthernet0/0), len
70, rcvd 3
*Mar  2 05:25:19:     UDP src=434, dst=434
MobileIP: FA received MN failed authentication (131) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01A08 end 3B01A1E
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
```

No IRDP on Foreign Agent Interface

This debug example shows where ICMP Router Discovery Protocol (IRDP) is not configured on the foreign agent interface. It shows the ARP process reacting to the mobile nodes address when it tries to put it in the ARP table. The router adds the mobile node address in the ARP table when it sends a registration request or an ip IRDP solicitation. In either case, IRPD must be enabled on the foreign agent interface.

On the Foreign Agent:

```
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
MobileIP: FastEthernet1/0 add 10.0.150.200 rejected
 (repeated …)
```

No IRDP on Home Agent Interface

This debug example shows where IRDP is not configured on the home agent interface. On the home agent, the interface continues to receive solicitations from the Mobile IP client. Unlike the foreign agent, there are no ARPing errors because the host is on the correct subnet.

On the Home Agent:

```
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
*Mar  1 03:56:35:     ICMP type=9, code=0
*Mar  1 03:56:35: IP: s=10.0.150.200 (FastEthernet0/0), d=10.0.150.6, len 74, rcvd 0
```

Time Clocks Not Synchronized on Mobile Node and Home Agent

This debug example shows the clock of the Mobile IP client is not within the specified variance of the home agent clock. The identification field in the registration reply holds the clock of the mobile node when the clock does not match the home agent clock. The registration request is rejected and the home agent sends a reply with the offset between the clocks on the mobile nodes and home agent clock. The mobile node corrects its timestamp in the next registration request, so it matches the home agent clock.

On the Home Agent:

```
MobileIP: HA 91 received registration for MN 10.0.150.200 on FastEthernet0/0 using COA
193.1.1.1 HA 10.1.1.1 lifetime 300 options sbdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D06
MobileIP: Skip2TLV look 32 != type 200, addr FA36CEC end FA36D06
MobileIP: Skip2TLV skipping 2
MobileIP: Skip2TLV look for type 32, addr start FA36D06 end FA36D06
MobileIP: MN 10.0.150.200 - authenticating MN 10.0.150.200 using SPI 100
MobileIP: MN 10.0.150.200 - authenticated MN 10.0.150.200 using SPI 100
MobileIP: Identification field 970198610 has timestamp 1969734999 secs less than our
current time 03/01/93 00:13:29 2939933609 (< allowed 255 secs) for MN 10.0.150.200
*Feb 28 16:13:29: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.150.200 -
errcode registration id mismatch (133), reason Bad identifier (3)
MobileIP: HA rejects registration for MN 10.0.150.200 - registration id mismatch (133)
MobileIP: MN 10.0.150.200 - MH auth ext added (SPI 100) to MN 10.0.150.200
MobileIP: MN 10.0.150.200 - HA sent reply to 172.1.1.2
```

On the Foreign Agent:

```
*Feb 28 16:07:17:
MobileIP: Agent advertisement sent out FastEthernet0/1: type=16, len=10, seq=38,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Feb 28 16:07:17: Care-of address: 193.1.1.1
MobileIP: FA received registration for MN 10.0.150.200 on FastEthernet0/1 using COA
193.1.1.1 HA 10.1.1.1 lifetime 300 options sbdmgvt
MobileIP: FA queued MN 10.0.150.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.150.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3CB5CEC end 3CB5D06
MobileIP: Skip2TLV look 32 != type 200, addr 3CB5CEC end 3CB5D06
MobileIP: Skip2TLV skipping 2
MobileIP: FA forwarded registration for MN 10.0.150.200 to HA 10.1.1.1
MobileIP: FA received registration id mismatch (133) reply for MN 10.0.150.200 on
FastEthernet0/0 using HA 10.1.1.1 lifetime 300
MobileIP: Skip2TLV look for type 32, addr start 3CB5CE8 end 3CB5CFE
MobileIP: FA forwarding reply to MN 10.0.150.200 using src 10.0.150.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.150.200 from register table
*Mar  1 03:56:36: IP ARP: rcvd rep src 10.0.150.200 0010.a403.1357, dst 10.0.150.200
FastEthernet0/0
```

Missing ip mobile virtual-network Command on the Home Agent

This section shows an example of a configuration error on the home agent. Other configuration errors return the same code (128). Some errors cause the home agent not to respond with a registration reply. One of those is a missing security association for the mobile node.

On the Home Agent:

```
MobileIP: HA 92 received registration for MN 10.0.148.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: Skip2TLV look for type 32, addr start FA36CEC end FA36D02
MobileIP: Skip2TLV look for type 32, addr start FA36D02 end FA36D02
MobileIP: MN 10.0.148.200 - authenticating MN 10.0.148.200 using SPI 100
MobileIP: MN 10.0.148.200 - authenticated MN 10.0.148.200 using SPI 100
MobileIP: Request from MN 10.0.148.200 denied, no virtual network 10.0.148.0
MobileIP: HA rejects registration for MN 10.0.148.200 - reason unspecified (128)
MobileIP: MN 10.0.148.200 - MH auth ext added (SPI 100) to MN 10.0.148.200
MobileIP: MN 10.0.148.200 - HA sent reply to 10.0.150.5
```

On the Foreign Agent:

```
*Mar 16 21:48:37: ICMP: rdp solicit rcvd type 10, code 0, from 10.0.148.200
MobileIP: FastEthernet1/0 glean 10.0.148.200 accepted
*Mar 16 21:48:37:
MobileIP: Agent advertisement sent out FastEthernet1/0: type=16, len=10, seq=27734,
lifetime=36000, flags=0x1400(rbhFmGv-rsv-),
*Mar 16 21:48:37: Care-of address: 192.1.1.1
*Mar 16 21:48:37: ICMP: src=192.1.1.1, dst=10.0.148.200, irdp advertisement sent
*Mar 16 21:48:37: IRDP: entries=1, size=2, lifetime=180, bytes=48
*Mar 16 21:48:37: IRDP: address=192.1.1.1 preference=0
MobileIP: FA received registration for MN 10.0.148.200 on FastEthernet1/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: FastEthernet1/0 glean 10.0.148.200 accepted
MobileIP: FA queued MN 10.0.148.200 in register table
MobileIP: Visitor registration timer started for MN 10.0.148.200, lifetime 15
MobileIP: Skip2TLV look for type 32, addr start 3B0178C end 3B017A2
MobileIP: FA forwarded registration for MN 10.0.148.200 to HA 10.0.150.6
MobileIP: FA received reason unspecified (128) reply for MN 10.0.148.200 on
FastEthernet0/0 using HA 10.0.150.6 lifetime 36000
MobileIP: Skip2TLV look for type 32, addr start 3B01788 end 3B0179E
MobileIP: FA forwarding reply to MN 10.0.148.200 using src 10.0.148.200 mac 0010.a403.1357
MobileIP: FA dequeued MN 10.0.148.200 from register table
```

Mobile Node Is Not On Line

In this example, the mobile node is not online.

On the Home Agent:

```
MobileIP: MN 10.0.148.1 is offline, icmp unreachable sent to sender 10.0.150.5
*Mar 16 20:31:59: ICMP: dst (10.0.148.1) host unreachable sent to 10.0.150.5
```

No Security Association for the Mobile Node on the Home Agent

In this example, nothing is sent back to a foreign agent, no registration reply, no ICMP unreachable. The registration request is completely ignored.

On the Home Agent:

```
MobileIP: HA 91 received registration for MN 10.0.148.200 on FastEthernet0/0 using COA
192.1.1.1 HA 10.0.150.6 lifetime 36000 options sBdmgvt
MobileIP: MN 10.0.148.200 SA is not configured, request ignored
*Feb 28 16:02:20: %IPMOBILE-6-SECURE: Security violation on HA from MN 10.0.148.200 -
errcode MN failed authentication (131), reason No mobility security association (1)
```

Configuration Register Modification

The virtual configuration register is in nonvolatile RAM (NVRAM) and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software.

Table 18-2 shows the software configuration bit descriptions.

Table 18-2 Software Configuration Bit Descriptions

Bit No.	Hex	Description
00-03	0x0000-0x000F	Boot Field (see Table 18-3)
06	0x0040	Ignore NVM contents
07	0x0080	OEM bit enabled
08	0x0100	Break disabled
10	0x0400	IP broadcast with all zeros
11-12	0x0800-0x1000	Console line speed
13	0x2000	Boot default ROM software if network boot fails
14	0x4000	IP broadcasts do not have net numbers
15	0x8000	Enable diagnostic messages and ignore NVM contents

Table 18-3 shows the boot field register bits.

Table 18-3 Explanation of Boot Field (Configuration Register Bits 00-03)

Boot Field	Meaning
00	Stays at the system bootstrap prompt
01	Boots system image on EPROM
02-F	Specifies a default netboot filename Enables boot system commands that override default netboot filename[1]

1. Values of the boot field are 2-15 in the form cisco<n>-processor_name, where 2 < n < 15.

The value is always interpreted as hexadecimal. Entering **confreg** without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

In either case, the new virtual configuration register value is written into NVRAM but does not take effect until you reset or reboot the router.

To change the virtual configuration register from the ROM monitor, enter **confreg** or enter the new value of the register in hexadecimal.

The following display shows an example of entering the **confreg** command:

```
rommon 2> confreg

Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable diagnostic mode? y/n  [n]:  y
enable use net in IP bcast address? y/n  [n]:
enable load rom after netboot fails? y/n  [n]:
enable use all zero broadcast? y/n  [n]:
enable break/abort has effect? y/n  [n]:
enable ignore system config info? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:

You must reset or power cycle for new config to take effect
```

Password Recovery

This section describes how to recover a password that you configured with the **enable** command (enable password) on the Cisco 3200 Series router.

Note You can recover a lost enable password, but not a password that you configured with the **enable secret** command (enable secret password). This password is encrypted and must be replaced with a new enable secret password. See the "Hot Tips" section on Cisco Connection Online (CCO) for information on replacing enable secret passwords.

Follow these steps to recover a lost enable password:

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the Console port. For more information, see the "Terminal Configuration" section of the "Cisco 3200 Series Mobile Access Router Interfaces" chapter.

Step 2 Configure the terminal at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 Reboot the router.

Step 4 From user EXEC mode, display the existing configuration register value:

```
Router> show version
```

Step 5 Record the setting of the configuration register. The setting is usually 0x2102 or 0x102.

Step 6 Record the break setting.

- Break enabled—bit 8 is set to 0.
- Break disabled (default setting)—bit 8 is set to 1.

Note To enable break, enter the **config-register 0x01** global configuration command. The bit settings are described in Table 18-2.

Step 7 Turn off the power to the router and then turn it back on.

Step 8 Press **Break** on the terminal keyboard within 60 seconds of the power-up to put the router into ROMMON. The terminal displays the following prompt:

```
rommon 1>
```

Step 9 Reset the configuration register:

```
rommon 1> confreg 0x2142
```

Step 10 Initialize the router:

```
rommon 2> reset
```

The router reboots but ignores its saved configuration.

```
--- System Configuration Dialog ---
```

Step 11 Enter **no** in response to the prompts until the following message is displayed:

```
Press RETURN to get started!
```

Step 12 Press **Return**. The following prompt appears:

```
router>
```

Step 13 Enter privileged EXEC mode:

```
router> enable
```

The prompt changes to the privileged EXEC prompt:

```
router#
```

Step 14 Type **configure memory** or **copy startup-config running-config** to copy the nonvolatile RAM (NVRAM) into memory. Do not type configure terminal.

Step 15 Type **write terminal** or **show running-config**.

The **show running-config** and **write terminal** commands show the configuration of the router. In this configuration you see under all the interfaces the shutdown command, which means all interfaces are currently shutdown. Also, you can see the passwords (enable password, enable secret, vty, console passwords, and so on) either in encrypted or unencrypted format. The unencrypted passwords can be re-used, the encrypted ones will have to be changed with a new one.

Step 16 Type **configure terminal**.

```
router# configure terminal
hostname(config)#
```

Step 17 Type **enable secret** *password* to change the enable secret password, for example:

```
hostname(config)#enable secret cisco
```

Step 18 Issue the **no shutdown** command on every interface that is used. If you issue a **show ip interface brief** command, every interface that you want to use should be "up up".

Step 19 Type config-register 0x2102, or the value that you recorded in Step 5.

```
router# config-register value
```

Step 20 Press **Ctrl-Z** to exit configuration mode.

Step 21 Type **write memory** or **copy running-config startup-config** to commit the changes.

Step 22 Reboot the router, and enter the recovered password.