Release Notes for Cisco MWR 1941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(15)MC1

September 15, 2003

Cisco IOS Release 12.2(15)MC21

OL-13984-06

These release notes are for the Cisco MWR 1941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(15)MC1. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

For a list of the software caveats that apply to Cisco IOS Release 12.2(15)MC1, see the "Caveats in Cisco IOS Release 12.2(15)MC1" section on page 9. To review the release notes for Cisco IOS Release 12.2, go to www.cisco.com and click **Technical Documents**. Select **Release 12.2** from the Cisco IOS Software drop-down menu. Then click **Cisco IOS Release Notes** > **Cisco IOS Release 12.2**.

Contents

This document contains the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco MWR 1941-DC Mobile Wireless Edge Router running Cisco IOS Release 12.2(8) MC2 or a later Cisco IOS 12.2 MC software release is a networking platform optimized for use in mobile wireless networks. It extends IP connectivity to the cell site and Base Transceiver Station (BTS), and through a Fast Ethernet interface to the BTS, provides bandwidth-efficient IP transport of voice and data bearer traffic, as well as maintenance, control, and signalling traffic, over the leased line backhaul network between the BTS and leased line termination and aggregation node via compression (cRTP/cUDP) and packet multiplexing (PPPMux and MLPPP). It supports a limited set of interfaces and protocols, but offers high performance at a low cost while meeting the critical requirements for deployment in cell sites, including small size, extended operating temperature range, high availability, and DC input power flexibility.

System Configuration Requirements

The Cisco MWR 1941-DC Mobile Wireless edge router requires the following system configuration:

- Cisco IOS 12.2(8) MC2 or a later Cisco IOS Release 12.2 MC software be installed.
- Network Time Protocol (NTP)

  Network Time Protocol must be configured. The Cisco MWR 1941-DC router uses NTP to maintain a clocking source for the proper time stamping of system messages and log files.
- Redundancy

  When not using the Cisco MWR 1941-DC router in a redundant configuration, the standalone option must be configured from redundancy mode.

  When using the Cisco MWR 1941-DC router in a redundant configuration:

  - Keepalives under the FE must be set to 1.
  - Extended Availability Drop and Insert (EADI) capabilities must be disabled on the router (using the **disable-eadi** global configuration command) to avoid a double-termination situation upon router reboot. If the MWR 1941-DC is not being used in a redundant configuration and EADI is specifically required, you can re-enable EADI using the **no disable-eadi** global configuration command.
  - When attaching the MWR 1941-DC to a device that uses spanning tree, portfast must be configured on the device to avoid problems with HSRP at startup.

- Cisco Express Forwarding (CEF)

  You cannot disable Cisco Express Forwarding (CEF) on the MWR 1941-DC. Commands such as **no ip cef** will display an error message "%Cannot disable CEF on this platform." Some commands, such as **no ip route-cache cef**, will not return an error message, however, CEF will not be disabled regardless of whether or not an error message is displayed.

- Hot Standby Router Protocol (HSRP)

  In case of a tie in priority, HSRP uses the IP address to determine the active router. Therefore, you should ensure that the order of the IP addresses of the E1/T1 interfaces of the active router corresponds to the order of the IP addresses of the E1/T1 interfaces of the standby router.

Memory Recommendations

Table 1 Memory Recommendations for the Cisco MWR 1941-DC Mobile Wireless Edge Router

Platform	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWR 1941-DC Mobile Wireless Edge Router	mwr1900-i-mz	32 MB Flash	128 MB DRAM	RAM

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco MWR 1941-DC router, log in to the Cisco MWR 1941-DC and enter the **show version** EXEC command:

```
router> show version
     Cisco Internetwork Operating System Software
     IOS (tm) 1900 Software (MWR1900-I-MZ), Version 12.2(8)MC2, EARLY DEPLOYMENT RELEASE
     SOFTWARE (fc1)
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to Software Installation and Upgrade Procedures located at the following URL:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Upgrading to a New ROM Monitor Version

The Cisco MWR 1941-DC router ROM Monitor (ROMMON) consists of two modules:

- A resident module that is not changed during the upgrade procedure.
- An upgradable module that is updated during the upgrade procedure. This is the only module that you will download from Cisco.com.

Note Before performing this procedure, you must download the new ROMMON image from Cisco.com. The download procedure is the same as downloading Cisco IOS software images.

Note In the event of a power outage, the ROM monitor download will not be successful.

Note Command output is similar to the following.

To upgrade the ROMMON version on your Cisco MWR 1941-DC router, complete these steps from EXEC mode:

Step 1 Copy the new ROMMON image from a TFTP server to slot0.

Step 2 Verify that the new image has been copied:

```
Router#dir slot0:
  Directory of slot0:/
  3 -rw- 871 Mar 01 1993 00:05:02 MWR1900-3-default.cfg
  4 -rw- 610704 Mar 01 1993 00:10:30 MWR1900_RM2.srec.122-8r.MC3
```

Step 3 Upgrade the current configuration by entering the **upgrade rom-monitor** command as shown in the following example:

```
Router# upgrade rom-monitor file slot0:MWR1900_RM2.srec.122-8r.MC3
This command will reload the router. Continue? [yes/no]:y
```

Step 4 Press **Enter** to continue. The router begins downloading the ROMMON image. The router automatically reboots.

```
ROMMON image upgrade in progress
Erasing boot flash
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Programming boot flash pppp

Now Reloading
System Bootstrap, Version 12.2(20010915:181836) DEVELOPMENT SOFTWARE
Copyright (c) 1994-2001 by cisco Systems, Inc.

 Running new upgrade for first time

System Bootstrap, Version 12.2(8r)MC3, RELEASE SOFTWARE (fc1)
TAC Support:http://www.cisco.com/tac
Copyright (c) 2002 by cisco Systems, Inc.
mwr1900 processor with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Upgrade ROMMON initialized
rommon 1 >
```

New Features in the Cisco IOS Release 12.2(15)MC1 Software

The following new features are introduced in Cisco IOS Release 12.2(15)MC1:

- Ignoring the IP ID in RTP/UDP Header Compression, page 5
- Configuring ACFC and PFC Handling During PPP Negotiation, page 5
- Configuring the cUDP Flow Expiration Timeout Duration, page 7

For information on new features in previous Cisco IOS Release 12.2MC software releases, see the platform release notes:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/ipran/1_0/relnotes/index.htm

Ignoring the IP ID in RTP/UDP Header Compression

With Cisco IOS Release 12.2MC2c, IP ID checking was suppressed in RTP/UDP header compression. With Cisco IOS Release 12.2(15)MC1 and later, a new option has been added to the **ip rtp header-compression** interface configuration command that allows you to enable or suppress this checking. The default is to suppress.

To suppress IP ID checking, issue the following command while in interface configuration mode:

Command	Purpose
`Router(config-if)# ip rtp header-compression ignore-id`	Suppresses the IP ID checking in RTP/UDP header compression.

To restore IP ID checking, use the **no** form of this command.

This new feature is identified by CSCdz75957.

Configuring ACFC and PFC Handling During PPP Negotiation

With Cisco IOS Release 12.2(15)MC1 and later, how ACFC and PFC are processed during PPP negotiation can be configured.

Configuring ACFC Handling During PPP Negotiation

Use the following commands beginning in global configuration mode to configure ACFC handling during PPP negotiation:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# shutdown`	Shuts down the interface.

	Command	Purpose
Step 3	`Router(config-if)# ppp acfc remote {apply | reject | ignore}`	Configures how the router handles the ACFC option in configuration requests received from a remote peer. • **apply**—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • **reject**—ACFC options are explicitly ignored. • **ignore**—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.
Step 4	`Router(config-if)# ppp acfc local {request | forbid}`	Configures how the router handles ACFC in its outbound configuration requests. • **request**—The ACFC option is included in outbound configuration requests. • **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.
Step 5	`Router(config-if)# no shutdown`	Reenables the interface.

Configuring PFC Handling During PPP Negotiation

Use the following commands beginning in global configuration mode to configure PFC handling during PPP negotiation:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# shutdown`	Shuts down the interface.
Step 3	`Router(config-if)# ppp pfc remote {apply | reject | ignore}`	Configures how the router handles the PFC option in configuration requests received from a remote peer. • **apply**—PFC options are accepted and PFC may be performed on frames sent to the remote peer. • **reject**—PFC options are explicitly ignored. • **ignore**—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.

	Command	Purpose
Step 4	`Router(config-if)# ppp pfc local {request	forbid}`	Configures how the router handles PFC in its outbound configuration requests. • **request**—The PFC option is included in outbound configuration requests. • **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.
Step 5	`Router(config-if)# no shutdown`	Reenables the interface.

To restore the default, use the **no** forms of these commands.

Note For complete details of the ACFC and PFC Handling During PPP Negotiation feature, see the *ACFC and PFC Handling During PPP Negotiation* feature module:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_15/12b_acf.htm#1025043

Configuring the cUDP Flow Expiration Timeout Duration

To minimize traffic flow corruption, cUDP flows now expire after an expiration timeout duration during which no packets are passed. When this duration of inactivity occurs on a flow at the compressor, the compressor sends a full header upon receiving a packet for that flow, or, if no new packet is received for that flow, makes the CID for the flow available for new use. When a packet is received at the decompressor after the duration of inactivity, the packet is dropped and a context state message is sent to the compressor requesting a flow refresh.

The default expiration timeout is 5 seconds. The recommended value is 8 seconds.

Caution Failure of performance/latency scripts could occur if the expiration timeout duration is not changed to the recommended 8 seconds.

To configure the cUDP flow expiration timeout duration, issue the following command while in multilink interface configuration mode:

Command	Purpose
`Router(config-if)# ppp iphc max-time seconds`	Specifies the duration of inactivity, in seconds, that when exceeded causes the cUDP flow to expire. The recommended value is 8.

To restore the default, use the **no** form of this command.

This new feature is identified by CSCeb44623.

Limitations, Restrictions, and Important Notes

Caution The Cisco MWR 1941-DC router does not support online insertion and removal (OIR) of WAN interface cards. Any attempt to perform OIR on a card in a powered up router might cause damage to the card.

Caution Removing the compact flash from the Cisco MWR 1941-DC router during a read/write operation might corrupt the contents of the compact flash, rendering it useless. To recover from an accidental removal of or corruption to the compact flash, a maintenance spare with the appropriate bootable Cisco IOS software image might be needed.

Unsupported Cisco IOS Software Features

The Cisco MWR 1941-DC router requires a special version of Cisco IOS software. Not all Cisco IOS software features can be used with the Cisco MWR 1941-DC router as the core routing is handled by the network processor. The following standard Cisco IOS software features are not supported on the Cisco MWR 1900 router:

- Security Access Control Lists
- MPLS
- 802.1Q VLANs
- Frame Relay (FR)
- MLP LFI
- ATM

Upgrading the VWIC-2MFT-T1-DIR Microcode

When upgrading the image on your Cisco MWR 1941-DC router, power cycle the router or perform a microcode reload on the VWIC-2MFT-T1-DIR to ensure that the firmware for the VWIC-2MFT-T1-DIR is updated during the upgrade.

Disabling PPP Multiplexing

To fully disable PPP multiplexing (PPPMux), issue the **no ppp mux** command on the T1 interfaces of the routers at both ends of the T1 link. If PPP multiplexing remains configured on one side of the link, that side will offer to receive PPP multiplexed packets.

MLP LFI Support

MLP LFI is not supported by the Cisco MWR 1941-DC router. Therefore, MLP LFI must be disabled on peer devices connecting to the Cisco MWR 1941-DC router T1 MLP connections.

ACFC and PFC Support on PPP Interfaces

If upgrading to Cisco IOS Release 12.2(8)MC2c or later for the ACFC and PFC support on PPP interfaces, ensure that you upgrade the MGX-RPM-1FE-CP backcard image first. After doing so, immediately upgrade all MWR 1941-DC routers connected to the MGX-RPM-1FE-CP back card.

Caveats in Cisco IOS Release 12.2(15)MC1

The following sections list and describe the open and closed caveats for the Cisco MWR 1941-DC router running Cisco IOS Release 12.2(15)MC1. Only severity 1 through 3 caveats are included.

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(15)MC1. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T.* These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco Bugtool Navigator II**. Another option is to go directly to http://www.cisco.com/support/bugtools.

Open Caveats

The caveats listed in this section are open in Release 12.2(15)MC1.

- CSCdw34503

  When using an extended ACL with the **access-group** command to define traffic using the **class** policy-map configuration command, the Cisco MWR 1941-DC router crashes to ROMmon. This condition happens because extended ACLs are currently not supported.

  Workaround: The **access-group** command is not part of the IP-RAN configuration. However, if using the command, use only with standard ACLs.

- CSCdw56881

  When traffic shaping is applied to an MLP output interface, the shaped output rate might be slightly higher than that defined. This condition occurs because the data rate to that interface is greater than the shaping rate.

  Workaround: There is currently no workaround.

- CSCdy28494

  During periods of heavy multicast traffic (approximately 5000 pps), some multicast packets are dropped at the MWR 1941-DC MLP interface.

  Workaround: Reduce the rate of multicast traffic.

- CSCdz37497

  When PPPMux and cUDP are configured, during periods of sustained multicast traffic at a rate of 100 pps or more causes a periodic “out-of-sequence” condition in the MWR 1941-DC IOS decompression.

  Workaround: Reduce the rate of multicast traffic.

- CSCdz48133

  Periods of sustained mixed traffic (UDP multicast, IP, and TCP) might cause the MWR 1941-DC router to crash.

  Workaround: There is currently no workaround.

- CSCin49064

  ifOperStatus displays an incorrect value for PPP encapsulated serial interfaces. The serial interface and line protocol are up (verified issuing the show interfaces serial command), however, the ifOperStatus is displayed as “notPresent(6)” instead of “up(1)”.

  Workaround: There is currently no workaround.

- CSCin51913

  Because they are not populated correctly, the cHsrpExtIfTrackedTable and cHsrpExtIfTable return null values when queried.

  Workaround: Issue the show standby fastEthernet 0/0 command on the MWR 1941-DC router.

Closed or Resolved Caveats

This section lists the caveats that are closed or resolved in Release 12.2(15)MC1.

- CSCdx85735

  When the class-default queue is used with other class-based queues, the class-default queue’s committed information rate (CIR) and the excess information rate are not configured correctly.

- CSCdy09568

  QoS class-based WFQs configured with a low percentage of bandwidth cannot use the unused bandwidth from queues assigned a high percentage of the bandwidth.

- CSCdy31030

  Entering or modifying the **shape** class-map configuration command to a policy map that has already been applied to an interface has no affect. Therefore, there will be no change to the traffic flow for that class of traffic. In addition, specifying certain values using the **shape** command might generate the message “Shape rate too low for *interface*.”

- CSCdy74371

  After a PXF crash on the MWR 1941-DC router and the PXF is restarted, traffic flowing over the bundle is sent with two MLP headers. The aggregation router will drop all received traffic. This condition does not affect traffic flowing from the bundle to the FE interface.

- CSCdz21464

  The Cisco MWR 1941-DC router will enclose the host name within quotes in the configuration if the **hostname** *hostname* command is configured.

- CSCdz23375

  When PPPMux and cUDP are configured, UDP fragmentation at traffic rates of 600 pps or more causes conditions such as dropped packets at the receiving MLP interface and tail drops at the receiving FE interface.

- CSCdz45713

  Tail drops and output queue drops occur at traffic rates of mixed traffic of 6000 pps over a 4 T1 WAN link.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea10513

  The Line Error Seconds counter under the VWIC-MFT **show controller t1/e1** command output keeps incrementing when switched to UnAvailable Seconds after 10 Severely Errored Seconds.

- CSCea73056

  During a failover, the MWR 1941-DC router software opens T1/E1 relays on the active router without taking down the multilink interface first. Packets are sent to the disconnected interface for the next several second until the multilink interface is declared down. This condition causes the network management system to not receive SNMP traps generated during the failover.

- CSCeb00369

  The MWR 1941-DC router might crash during channel-group provisioning.

- CSCeb17244

  All multicast traffic outbound to the MLP interface is incorrectly scheduled for only one of the 4 T1s which are active members of the bundle. This condition causes multicast traffic above that one T1's bandwidth to be dropped.

- CSCeb37865

  When Qmax is set to an arbitrary number (non power of 2), it is being set to the closest power of 2 rather than the smallest power of 2 to sufficient to support the Qlimit.

- CSCeb43906

  When sending non PXF-handled traffic (for example, uncompressed, unfragmented, non-multicast Fast Ethernet traffic) the Fast Ethernet total input byte count is incorrect.

- CSCeb78926

  When configuring a T1 channel group, serial interfaces appear fine, MLP interface is UP/UP, but there is no WAN connectivity.

- CSCin16619

  Upon deleting a channel group, tracebacks might occur at "process_ok_to_reschedule" and traffic might not pass through even though the interface is up and the routes exist.

- CSCin31634

  SNMP query of ciscoFlashDeviceSize returns 0.

- CSCin32105

  The cardSerial and cardSlots MIB variables display the wrong values.

Troubleshooting

Collecting Data for Router Issues

To collect data for reporting router issues, issue the following command:

- **show tech-support**—Displays general information about the router when it reports a problem.

Collecting Data for Redundancy Issues

To collect data for redundancy-related issues, issue the following commands while in EXEC mode:

- **show cdp neighbors**—Displays detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP).
- **show controllers**—Displays information that is specific to the hardware.
- **show ip interface**—Displays the usability status of interfaces configured for IP.
- **show redundancy**—Displays current or historical status and related information on redundant Dial Shelf Controllers (DSCs).
- **show standby**—Displays Hot Standby Router Protocol (HSRP) information.
- **show standby brief**—Displays Hot Standby Router Protocol (HSRP) information; specifically, with the brief keyword specified, a single line of output summarizing each standby group.

Collecting Data for ROMmon Issues

To collect data for ROMmon issues, issue the following command while in EXEC mode:

- **showmon**— Displays currently selected ROM monitor.

Collecting Data for Router Rebooting to ROMmon

If a router reboot to ROMmon occurs, issue the **dir** *device ID* command where *device ID* is slot0:, and look for the router processor or network processor exception file (crashinfo* or pxf_crashinfo* respectively). Once you have located one of these files, you can email the file along with a description of the problem to your Cisco representative.

Documentation Updates

The following sections describe updates to the published documentation for the Cisco MWR 1941-DC Mobile Wireless edge router. The heading in this section corresponds with the applicable section title in the documentation.

Configuring RTP/UDP Compression

The maximum number of RTP header compression connections per MLP bundle is documented as 600 when in fact, up to 1000 connections are supported on an interface. This change also applies to the **ip rtp header-compression** command description.

The show ip rtp header-compression Command

The **detail** keyword is not supported in the **show ip rtp header-compression** command. Therefore, output does not display for the `detail` keyword if it is specified in command.

Configuring T1 Interfaces

Some configuration modes shown in the procedure for configuring T1 interfaces in the "Configuring T1 Interfaces" of the *Cisco MWR 1900 Software Configuration Guide* are incorrect. The correct command modes are as follows:

Step 1 Specify the controller that you want to configure. For information about interface numbering, see the *Understanding Interface Numbering* section.

```
Router(config)# controller t1 slot/port
```

Step 2 Specify the framing type.

```
Router(config-controller)# framing esf
```

Step 3 Specify the line code format.

```
Router(config-controller)# linecode b8zs
```

Step 4 Specify the channel group and time slots to be mapped. For the VWIC interfaces, you can configure two channel-groups (0 and 1) on the first T1 port or you can configure one channel-group (0 or 1) on each T1 port. Once you configure a channel group, the serial interface is automatically created.

Note The default speed of the channel group is 56. To get full DS0/DS1 bandwidth, you must configure a speed of 64.

```
Router(config-controller)# channel-group 0 timeslots 1-24 speed 64
```

Step 5 Configure the cable length.

```
Router(config-controller)# cablelength feet
```

Note Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Step 6 Exit controller configuration mode.

```
Router(config-controller)# exit
```

Step 7 Configure the serial interface. Specify the T1 slot (always 0), port number, and channel group.

```
Router(config)# interface serial slot/port:0
```

Step 8 Assign an IP address and subnet mask to the interface. If the interface is a member of a Multilink bundle (MLPPP), then skip this step.

```
Router(config-if)# ip address ip_address subnet_mask
```

Step 9 Before you can enable RTP header compression, you must have configured a serial line that uses PPP encapsulation. Enter the following command to configure PPP encapsulation.

```
Router(config-if)# encapsulation ppp
```

Step 10 Set the carrier delay for the serial interface.

```
Router(config-if)# carrier-delay number
```

Step 11 Return to Step 1 to configure the second port on the VWIC and the ports on any additional VWICs.

Step 12 Exit to global configuration mode.

```
Router(config-if)# exit
```

Configuring Redundancy

Before configuring redundant MWR 1941-DC routers as described in the "Configuring T1 Interfaces" section of the *Cisco MWR 1900 Software Configuration Guide*, ensure that you disable EADI capabilities on the router by issuing the **disable-eadi** global configuration command as follows:

```
Router(config)# disable-eadi
```

Related Documentation

The following sections describe the documentation available for the Cisco MWR 1941-DC Mobile Wireless Edge Router. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Platform-Specific Documents

These documents are available for the Cisco MWR 1941-DC Mobile Wireless Edge Router on Cisco.com and the Documentation CD-ROM:

- Cisco MWR 1941-DC Mobile Wireless Edge Router
  - *Cisco MWR 1941-DC Hardware Installation Guide*
  - *Cisco MWR 1900 Software Configuration Guide*
  - *Cisco MWR 1941-DC Rack Mounting Instructions*
  - *Cisco MWR 1941-DC Regulatory Compliance and Safety Information*
- *VWIC-2MFT-T1-DIR, VWIC-2MFT-E1-DIR Installation Instructions*
- *MGX-RPM-1FE-CP Back Card Installation and Configuration Note*

On Cisco.com at:

Technical Documents: Cisco Product Documentation: Fixed and Mobile Wireless Solution: Cisco Mobile Wireless IP-RAN: Cisco Mobile Wireless IP-RAN Version 1.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Fixed and Mobile Wireless Solution: Cisco Mobile Wireless IP-RAN: Cisco Mobile Wireless IP-RAN Version 1.0

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2 MC and are updates to the Cisco IOS documentation set. A feature module consists of an overview of the feature, configuration tasks, and a command reference.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in Release 12.2 MC: New Features in Release 12.2 MC2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in Release 12.2 MC: New Features in Release 12.2 MC2

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.