Release Notes for Cisco MWR 1900 Mobile Wireless Edge Router for Cisco IOS Release 12.2(8)MC2d

March 17, 2003

Cisco IOS Release 12.2(8)MC2d

OL-13984-05

These release notes are for the Cisco MWR 1900 Mobile Wireless Edge Router for Cisco IOS Release 12.2(8)MC2d. 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(8)MC2d, see the "Caveats in Cisco IOS Release 12.2(8)MC2d" section on page 11. 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:

CISCO SYSTEMS

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

Introduction

The Cisco MWR 1900 Mobile Wireless Edge Router running Cisco IOS Release 12.2(8) MC2 or a later Cisco IOS Release 12.2 MC 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 1900 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 1900 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 1900 router in a redundant configuration, the standalone option must be configured from redundancy mode.

When using the Cisco MWR 1900 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 1900 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 1900 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 1900. 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 1900 Mobile Wireless Edge Router

Platform	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWR 1900 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 1900 router, log in to the Cisco MWR 1900 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 MWR 1900 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.

To upgrade the ROMMON version on your Cisco MWR 1900 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
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
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 MC Software

The following sections list the new hardware and software features supported by the Cisco MWR 1900 router for the Cisco IOS Release 12.2MC software releases:

New Features in Cisco IOS Release 12.2(8)MC2

For detailed descriptions of each of these features, see the *Cisco MWR 1900 Mobile Wireless Edge Router Software Configuration Guide*.

With Cisco IOS Release 12.2(8)MC2, the MWR 1900 router supports the following:

- Cisco IOS Software Features

  Cisco IOS software function added for the Cisco MWR 1900 router IP-RAN application include:

  - Redundancy logic
  - Failover logic
  - Relay control
  - Diagnostic functions

  Standard Cisco IOS software features supported in this release include:

  - IP Fragmentation
  - IP Multicast
  - IGMP
  - MLP, PPP Control Path (IPCP, NCP, LCP, CLNS)
  - HSRP
  - OSPF
  - DHCP
  - CDP
  - NTP
  - SNMP

- Network Processor Software

  The following features are supported in the network processor:

  - MAC Classify
  - ICMP
  - FIB (CEF)
  - Load-balancing
  - MAC Rewrite
  - QoS Matching
  - QoS Actions
  - Statistic maintenance
  - IPv4
  - MLPPP, MLP, PPP Data Path (MLP LFI is not supported)
  - PPPMux
  - cRTP/cUDP

- Redundancy support

- Cisco Hot Standby Router Protocol (HSRP) support

- MIB support

New Feature in Cisco IOS Release 12.2(8)MC2b

The following new feature is introduced in Cisco IOS Release 12.2(8)MC2b.

Traffic Recovery Over MLP After T1 Failure

When a T1 failure occurs, traffic recovers over the MLP link within 6 seconds.

This caveat is a feature enhancement to the **keepalive** interface configuration command. With this enhancement, you can also configure a maximum number of retries before a link is declared down by issuing the command as follows:

> **keepalive** [*interval*] [*retries*]

where:

- *interval* is the keepalive interval (in seconds). Valid value is a number greater than 0. The default is 10.

- *retries* is the number of times a link will be tried again before being declared down. Valid value is a number between 1 and 255. The default is 5.

For implementation in an IP RAN solution, the recommended configuration is as follows:

On the MWR 1900:

```
interface Serial0/0:0
 no ip address
 encapsulation ppp
 keepalive 1 2
 no cdp enable
 ppp multilink
 multilink-group 1
end
```

On the MGX-RPM-1FE-CP back card;

```
interface Virtual-Template2
 bandwidth 1536
 no ip address
 keepalive 1 2
 no peer default ip address
 ppp multilink
 multilink-group 101
end.
```

Note   In the MGX-RPM-1FE-CP backcard configuration example, only the **keepalive** interface command and configuration recommendation is specific to implementation in an IP RAN solution.

This new feature is identified by CSCdy78207.

New Features in Cisco IOS Release 12.2(8)MC2c

The following new features are introduced in Cisco IOS Release 12.2(8)MC2c:

- ACFC and PFC Support on PPP Interfaces, page 7
- Ignore IP ID Field Delta in cUDP Packet Flows Support, page 7

ACFC and PFC Support on PPP Interfaces

By default, Address and Control Field Compression (ACFC) and Protocol Field Compression (PFC) are enabled on PPP interfaces. Both features are always enabled and will be negotiated on all serial interfaces.

Note If upgrading for this support, ensure that you upgrade the MGX-RPM-1FE-CP backcard images first. After doing so, immediately upgrade all MWR 1900 routers connected to the MGX-RPM-1FE-CP back card.

This new feature is identified by CSCdz15365.

Ignore IP ID Field Delta in cUDP Packet Flows Support

By default, the ability to ignore IP ID field delta in cUDP traffic flows is enabled. This ability eliminates the need to send information about the IP header ID field in compressed packets. The decompressor saves the original ID field from the full header packet and generates an ID field by incrementing it by one for each decompressed packet.

This feature improves processing efficiency; helping to minimize dropped packets and link saturation.

This feature is identified by CSCdz00521.

New Features in the Cisco IOS Release 12.2(8) MC2d Software

The following new features are introduced in Cisco IOS Release 12.2(8)MC2d:

- Link Noise Monitor, page 7
- Double cUDP Full Headers, page 10

Link Noise Monitor

Noise on T1 and E1 links that span between the BTS and central office can affect voice quality for mobile users to the point where it becomes unacceptable. Therefore, beginning with Cisco IOS Release 12.2(8)MC2d software, the Link Noise Monitor (LNM) can be configured on your MWR 1900 router.

The LNM monitors the quality of individual links in a multilink bundle and provides the ability to detect, alert, and remove noisy links from a bundle based on user-defined thresholds and durations. In addition, the LNM notifies the operator once the quality of the line has improved, and restores the link service if the link has been removed.

Specifically, to detect noise on a link, the LNM monitors the following two types of errors which make up the Bit Error Rate (BER) and compares the number of errors with the user-defined thresholds:

- Line Code Violation (LCV)—A Bi-Polar Violation (BPV) or Excessive Zeroes (EXZ) error has occurred.

- Path Code Violation (PCV)—A Cyclic Redundancy Check (CRC) error, which is generally caused by one or more LCV or logic errors, has occurred in a time slot.

The LNM provides the following types of noise monitors:

- Link Warning—Issues a warning when the noise level of a link exceeds a user-defined threshold and notifies the operator when the noise level improves to the point that it drops below a second user-defined threshold.

- Link Removal—Issues an error and removes a link from service when the noise level of the link exceeds a user-defined threshold and restores the link and provides notification when the noise level improves to the point that it drops below a second user-defined threshold.

> **Note** If the noise level on the last active link in a multilink bundle exceeds the Link Removal threshold, an alert is issued but the link will not be removed from service. If this situation occurs, the standard T1 error rate is used to determine if the last active link must be removed from service.

Configuring LNM

To configure the LNM feature, issue the **span** command from controller configuration mode of each T1 or E1 link in the bundle that you want to monitor. To disable LNM on a link, issue the **no** version of the command from controller configuration mode of the link.

span { **warn** | **remove** } [{ [**lcv** *value* [**pcv** *value*]] [**duration** *seconds*] } **set** | **clear**]

where:

- **warn**—Enables Link Warning monitoring on the link.

- **remove**—Enables Link Removal monitoring on the link.

- **lcv** *value*—Threshold (in bit errors per second) that when exceeded for the configured duration when the **set** keyword has been specified, creates a condition (warning or link removal), or when fallen below for the configured duration when the **clear** keyword has been specified, clears the condition.

   For T1 links:

   - Valid range is 5 to 1544.

   - For Link Warning monitoring, the default is 15.

   - For Link Removal monitoring, the default is 154.

   For E1 links,

   - Valid range is 7 to 2048.

   - For Link Warning monitoring, the default is 20.

   - For Link Removal monitoring, the default is 205.

- **pcv** *value*—Number of time slots in errors per second. If not specified by the user, this value is calculated from the LCV threshold based on a Gaussian distribution that matches typical noise-induced errors.

For T1 links:

- Valid range is 3 to 320.
- For Link Warning monitoring, the default is 15.
- For Link Removal monitoring, the default is 145.

For E1 links,

- Valid range is 8 to 832.
- For Link Warning monitoring, the default is 20.
- For Link Removal monitoring, the default is 205.

- **duration** *seconds*—Number of seconds that a threshold must be exceeded to create a condition or fallen below to clear a condition. Valid range is 1 to 600. The default is 10.

  When specified with th**e lcv** keyword, the duration must be configured after the LCV threshold. For example, **span warn lcv 55 duration 20** is a correct way to issue the command; s**pan warn duration 20 lcv 55** is not.

- **set**—Specifies that the values configured for the **span** command are to be used to set a condition.

- **clear**—Specifies that the values configured for the **span** command are to be used to clear a condition.

LNM Usage Notes

When configuring the LNM, keep in mind the following:

- If the **warn** and **remove** keywords are specified without any other options, the LCV and PCV thresholds and duration defaults will be use to determine (**set**) and clear (**clear**) the condition.

- If the **span** command is issued with the **set** keyword specified (defining the LNM type and parameters to use to determine a condition exists) and the command is not issued again with the **clear** keyword specified (defining the parameters used to clear a condition), or vice versa, the values configured for the threshold and duration will be used for both.

- If the **span** command is issued without either the **set** or **clear** keywords specified, **set** is the default.

- The **set** and **clear** keywords can only be specified if the threshold and/or duration has been specified.

- If the PCV threshold is not configured (via the **pcv** keyword and value), the threshold is calculated using Gaussian probability distribution that is representative of most noise environments.

- The following SYSLOG messages have been added for fault notification:

  ```
  - %LNM-4- WARNEXCEED:Controller <Controller IF>, exceeded noise warning threshold
    <int>, duration <int>
  - %LNM-4- WARNIMPROVE:Controller <Controller IF>, noise improved below threshold
    <int>, duration <int>
  - %LNM-2-REMOVE:Interface <Serial IF> removed, noise exceeded threshold <int>,
    duration <int>
  - %LNM-2- RESTORE:Interface <Serial IF> restored, noise improved below threshold
    <int>, duration <int>
  - %LNM-2- REMEXCEED:Interface <Serial IF>, noise exceeded threshold <int>,
    duration <int>
  - %LNM-2- REMIMPROVE:Interface <Serial IF>, noise improved below threshold <int>,
    duration <int>
  ```

This new feature is identified by CSCdz84024.

Double cUDP Full Headers

At the start of a call flow, the MWR 1900 router and MGX 8850 RPM-PR back card now send the first two packets in the flow with full headers. This feature helps to minimize the loss of cUDP headers (and therefore misrouted packets) in noisy and/or congested networks.

This feature is identified by CSCdz84029.

Limitations, Restrictions, and Important Notes

⚠
Caution The Cisco MWR 1900 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 1900 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 1900 router requires a special version of Cisco IOS software. Not all Cisco IOS software features can be used with the Cisco MWR 1900 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 1900 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 1900 router. Therefore, MLP LFI must be disabled on peer devices connecting to the Cisco MWR 1900 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 1900 routers connected to the MGX-RPM-1FE-CP back card.

Caveats in Cisco IOS Release 12.2(8)MC2d

The following sections list and describe the open and closed caveats for the Cisco MWR 1900 router running Cisco IOS Release 12.2(8)MC2d. 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(8)MC2d. 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(8)MC2d.

- CSCdw34503

    When using an extended ACL with the **access-group** command to define traffic using the **class** policy-map configuration command, the Cisco MWR 1900 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.

- 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.

    Workaround: Manually configure the committed information rate using the **shape** class-map configuration command. The excess information rate cannot be manually configured, therefore, there is no workaround for it not configuring 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.

  Workaround: Deconfigure QoS on the output interface.

- CSCdy28494

  During periods of heavy multicast traffic (approximately 5000 pps), some multicast packets are dropped at the MWR 1900 MLP interface.

  Workaround: Reduce the rate of multicast traffic.

- 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*."

  Workaround: Remove the policy map from the interface and then reapply it, or save the new configuration and reload the router to get the changes to take effect. If the "Shape rate too low for *interface*" message displayed before, the value will be accepted and applied when one of the above methods is used.

- 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.

  Workaround: There is currently no workaround.

- 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 1900 IOS decompression.

  Workaround: Reduce the rate of multicast traffic.

- CSCdz45713

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

  Workaround: Reduce the UDP multicast packet rate to no more than 300 pps.

Closed or Resolved Caveats

This section lists the caveats that are closed or resolved in Release 12.2(8)MC2d

- CSCdy09568

  QoS class-based WFQs configured with a low percentage of bandwidth are unable to use the unused bandwidth from queues assigned a high percentage of the bandwidth.

- CSCdy23636

  When IOMEM is low, a PXF memory leak occurs when processing multicast traffic (into the FE and out the MLP interface).

- CSCdz84024

  Noise on T1 and E1 links spanning between the BTS site and central office causes errored packets to be dropped, resulting in degraded voice quality for mobile phone users.

  For more information about this resolved caveat, see the "Link Noise Monitor" section on page 7.

- CSCdz84029

  Noise, link overdrive, and other conditions might cause UDP packets to be lost or misrouted.

  For more information about this resolved caveat, see the "Double cUDP Full Headers" section on page 10.

- CSCdz87124

  While in standby mode, MWR 1900 router repeatedly sends T1 controller alarms for loss of signal (LOS) / loss of framing (LOF). However, when in standby mode, T1 controllers are electrically disconnected from the cable by relays and therefore should not be reporting any errors for they do not accurately represent the link state.

  This fix requires that you 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.

- CSCea15987

  During periods of high traffic, when UDP packets are compressed via RTP compression configured on a multilink bundle between the MWR 1900 router and the MGX-RPM-1FE-CP back card, some packets might be misrouted and have incorrect UDP checksums.

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 1900 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 1900s 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 1900 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 1900 Mobile Wireless Edge Router on Cisco.com and the Documentation CD-ROM:

- Cisco MWR 1900 Mobile Wireless Edge Router
  - *Cisco MWR 1900 Hardware Installation Guide*
  - *Cisco MWR 1900 Software Configuration Guide*
  - *Cisco MWR 1900 Rack Mounting Instructions*
  - *Cisco MWR 1900 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.