Release Notes for Cisco MGX-RPM-1FE-CP Back Card for Cisco IOS Release 12.2(15)MC1

September 15, 2003

Cisco IOS Release 12.2(15)MC1

OL-2920-06

These release notes are for the Cisco MGX-RPM-1FE-CP 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 MGX-RPM-1FE-CP (one-port, Fast Ethernet-Co-processor) back card is a Cisco MGX 8850 RPM-PR back card that off-loads the following processes from the Route Processor Module (RPM-PR):

- Compression/decompression of Real-time Transport Protocol (RTP)/User Datagram Protocol (UDP) headers (cRTP/cUDP)
- Multiplexing/demultiplexing of Point-to-Point Protocol (PPP) frames

The MGX-RPM-1FE-CP back card is designed to be used with an MGX 8850 that is equipped with one or more RPM-PRs and that terminates some number of T1 lines. Each MGX-RPM-1FE-CP back card has a termination capacity of up to 16 T1s (four per MLP bundle). The MGX-RPM-1FE-CP is only supported with the MLP encapsulation.

The MGX-RPM-1FE-CP back card contains one Fast Ethernet (100Base-Tx) interface. The interface has an RJ45 connector that is used to connect the card to a Category 5 un-shielded twisted pair (UTP) cable. Both half- and full-duplex operation are supported.

MGX-RPM-1FE-CP Back Card in an IP-RAN of a Mobile Wireless Network

The MGX-RPM-1FE-CP back card off loads the compression/decompression of RTP/UDP headers and the multiplexing/demultiplexing of PPP frames.

The supported use of the MGX-RPM-1FE-CP back card is within an IP-RAN of a mobile wireless network. In mobile wireless networks, radio coverage over a geographical space is provided by a network of radios and supporting electronics (Base Transceiver Station or BTS) distributed over a wide area. Each radio and supporting electronics represents a “cell.” In traditional networks, the radio signals or radio data frames collected in each cell are forwarded over a T1 (or similar low-speed, leased) line to a centralized Base Station Controller (BSC) where they are processed.

The implementation of the MGX-RPM-1FE-CP backcard in the IP-RAN solution requires the following components:

- Cisco MGX 8850
- RPM-PR
- MGX-RPM-1FE-CP back card
- FRSM card
- BTS router (Cisco MWR 1941-DC Mobile Wireless Edge Router)

The solution uses OSPF as the routing protocol and requires MLP for transmission of the packets between the aggregation node (MGX8850) and the BTS. It requires you to configure the following:

- The Fast Ethernet (FE) interface to support OSPF. Enable multicast routing and indicate a Protocol Independent Multicast (PIM) mode.
- One or more PPP multilink interfaces with PPP mux and RTP header compression attributes.
- A virtual template for each of the multilink groups.
- A PVC under the switch subinterface that references the virtual template.

In addition, you must configure a connection between the PVC and the FRSM as well as a connection between the FRSM and the PVC.

For detailed information about the MGX-RPM-1FE-CP back card and its implementation in the IP-RAN solution, see the *MGX-RPM-1FE-CP Back Card Installation and Configuration Note*.

System Configuration Requirements

The MGX-RPM-1FE-CP requires the following system configuration:

- Cisco IOS 12.2(8) MC1 or a later Cisco IOS Release 12.2 MC image is installed on the corresponding Cisco MGX 8850 RPM-PR.
- The FE interface is configured via the Cisco IOS software command line interface.

Memory Recommendations

Table 1 Memory Recommendations for the Cisco MGX 8850 RPM-PR

Platform	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MGX-RPM-1FE-CP	rpm-js-mz	32 MB Flash	256 MB DRAM	RAM

Determining the Software Version

To determine the version of Cisco IOS software copied on the RPM-PR, access the CLI of the RPM-PR and enter the **show version** command:

```
rpm> show version
     Cisco Internetwork Operating System Software
     IOS (tm) RPM Software (RPM-JS-M), Version 12.2(8)MC2, EARLY DEPLOYMENT RELEASE
     SOFTWARE (fc1)
```

Upgrading to a New Software Release

For information about copying Cisco IOS images to RPM-PR Flash memory, see the *RPM-PR Installation and Configuration* document.

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

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

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:

- Dual MGX-RPM-1FE-CP Back Card Support, page 4
- Ignoring the IP ID in RTP/UDP Header Compression, page 6
- Configuring ACFC and PFC Handling During PPP Negotiation, page 6
- Configuring the cUDP Flow Expiration Timeout Duration, page 8

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

Dual MGX-RPM-1FE-CP Back Card Support

With Cisco IOS Release 12.2(15)MC1 and later, support for a second MGX-RPM-1FE-CP back card is available. However, the second card functions as an FE interface only and does not perform any compression functions.

Usage Notes

Please note that when using two MGX-RPM-1FE-CP back cards in an RPM, the interaction between the two cards is as follows:

- When two MGX-RPM-1FE-CP back cards are installed in the RPM and the RPM boots or reboots, the card in the top slot always performs the compression function.
- When an MGX-RPM-1FE-CP back card is inserted via OIR, the slot with the first MGX-RPM-1FE-CP back card always performs the compression function.
- If two MGX-RPM-1FE-CP back cards are installed in an RPM and a card performing the compression function is removed via OIR, no compression functions will be active until one of the following events occurs:
  - a second MGX-RPM-1FE-CP back card is inserted
  - the remaining MGX-RPM-1FE-CP back card is removed and re-inserted
  - the RPM is rebooted
- Never remove a MGX-RPM-1FE-CP via OIR without shutting down all active interfaces on it. For a MGX-RPM-1FE-CP acting as a FE interface only, shut down just the FE port. For the back card performing the compression function, shut down the multilink bundles before removing.

Note This feature requires that the rpm-boot-mz image be upgraded so that the bootloader recognizes the second MGX-RPM-1FE-CP.

Additionally, the output of the **show diag** command has been updated to reflect the support for a second MGX-RPM-1FE-CP.

```
rpm10#sho diag
Slot 1:
 One Port Fast Ethernet With Co-processor Assist Port adapter, 1 port
 Port adapter is analyzed
 Port adapter insertion time 01:13:53 ago
 Co-processor enabled
 EEPROM contents at hardware discovery:
 Top Assy. Part Number :800-16088-04
 Part Number :73-6262-04
 Board Revision :02
 PCB Serial Number :PAD04001DHT
 CLEI Code :B@3@24Y@A@
 Manufacturing Engineer :00 00 00 00
 RMA History :00
 RMA Test History :00
 RMA Test History :02
 EEPROM format version 4
 EEPROM contents (hex):
 0x00:04 17 40 03 17 C0 46 03 20 00 3E D8 04 82 49 18
 0x10:76 04 42 30 32 C1 0B 50 41 44 30 34 30 30 31 44
 0x20:48 54 C6 8A 42 40 33 40 32 34 59 40 41 40 84 00
 0x30:00 00 00 04 00 03 00 03 02 FF FF FC FF FC FF FC
 0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Slot 2:
 ATM CELL BUS Port adapter, 1 port
 Port adapter is analyzed
 Port adapter insertion time 01:14:31 ago
 EEPROM contents at hardware discovery:
 Top Assy. Part Number :800-00000-00
 Part Number :73-0000-00
 Board Revision :0
 PCB Serial Number :0
 EEPROM format version 4
 EEPROM contents (hex):
 0x00:04 51 40 00 90 C0 46 03 20 00 00 00 00 82 49 00
 0x10:00 00 42 30 00 C1 01 30 FF FF FF FF FF FF FF FF
 0x20:09 40 C6 8A 30 00 00 00 00 00 00 00 00 00 84 00
 0x30:00 00 00 04 00 03 00 03 00 FF FF FF FF FF FF FF
 0x40:04 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x50:0A 2A FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x60:42 D2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x70:00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x80:09 03 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x90:42 82 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xA0:0C 83 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xB0:00 C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xC0:40 41 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xD0:82 82 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xE0:8C EC FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0xF0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x100:02 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x110:63 51 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x120:42 C2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x130:00 20 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x140:38 50 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x150:0C C2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x160:0C AC FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x170:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x180:62 C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x190:82 6C FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1A0:D1 CA FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1B0:00 C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1C0:92 C8 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1D0:21 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1E0:0C 8C FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x1F0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
Slot 3:
 One Port Fast Ethernet With Co-processor Assist Port adapter, 1 port
 Port adapter is analyzed
 Port adapter insertion time 01:14:07 ago
 Co-processor disabled
 EEPROM contents at hardware discovery:
 Top Assy. Part Number :800-16090-04
 Part Number :73-6518-04
 Board Revision :02
 PCB Serial Number :SAG06021EJ3
 CLEI Code :BA3A25YCAA
 Manufacturing Engineer :00 00 00 00
 RMA History :00
 RMA Test History :00
 RMA Test History :02
 EEPROM format version 4
 EEPROM contents (hex):
 0x00:04 17 40 03 17 C0 46 03 20 00 3E DA 04 82 49 19
 0x10:76 04 42 30 32 C1 0B 53 41 47 30 36 30 32 31 45
 0x20:4A 33 C6 8A 42 41 33 41 32 35 59 43 41 41 84 00
 0x30:00 00 00 04 00 03 00 03 02 FF FF FF FF FF FF FF
 0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
 0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

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.

Note By default, ACFC/PFC is not enabled and these commands must be configured on serial interfaces.

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.
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.

	Command	Purpose
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.
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

When working with a MGX-RPM-1FE-CP back card, please take note of the following limitations, restrictions, and important notes:

- Only one MGX-RPM-1FE-CP back card is supported per Cisco MGX 8850 RPM-PR.
- FE and multilink interfaces should be shut down before online insertion and removal (OIR) of the MGX-RPM-1FE-CP.
- The MGX-RPM-1FE-CP is only supported on the Cisco MGX 8850 RPM-PR.
- For PPP Multiplexing, MLP must be configured on the MGX-RPM-1FE-CP back card.
- For error messages to be stored, console logging must be configured.
- The IP MTU should be set to 512 bytes or less on multilink interfaces.
- The MGX-RPM-1FE-CP back card supports up to 16 multilink interfaces.
- MLP with LFI is not supported by the Cisco MWR 1941-DC router. Therefore, MLP with LFI must be disabled on peer devices connecting to the Cisco MWR 1941-DC router T1 MLP connections.
- To fully disable PPP Multiplexing, 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.
- 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 resolved caveats for the Cisco MGX-RPM-1FE-CP with 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

This section lists the caveats that are open in Release 12.2(15)MC1:

- CSCeb24086

  Administratively shutting down an FE interface while traffic is flowing on a second MGX-RPM-1FE-CP interface might cause a few seconds of packet lost on the second FE interface.

  Workaround: Do not administratively shut down an FE interface on an active system when traffic is flowing.
- CSCeb27247

  Disabling PPPmux on the RPM multilink interfaces causes from 1 to 4 serial links to stay down and the multilink to flap continuously.

  Workaround: Reset the RPMs switch subinterfaces experiencing this condition.
- CSCeb76514

  The checkheaps process detects corrupted memory and when packets back up into the bundle output hold queue, causes a router reload.

  Workaround: A software workaround (CSCeb74020) is implemented in the 12.2(15)MC1.

Resolved Caveats

This section lists the caveats resolved in Release 12.2(15)MC1.

- CSCdv73786

  In the case of a misconfiguration, the router might set the next hop to reach a forwarding address incorrectly.
- CSCdz21464

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

- 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

- CSCea25144 (duplicated by CSCea25124)

  RPM-PR card resets by PXM because of heartbeat failure.

- CSCea31579

  In an RPM-to-RPM multilink bundle with a single active member link on which cRTP is configured, periods of heavy compressed traffic with continuously changing flows might cause UDP checksum errors to occur on some decompressed packets.

- CSCea73441

  In a cell-based MPLS setup, if RPM-PR is receiving very high (99% OC3) traffic, the path check feature, which runs periodically may cause a memory corruption followed by a router reload.

- CSCeb22233

  Newly activated RPM in a 1:*n* redundant pair resets upon switchover.

- CSCeb23203

  Removing a MGX-RPM-1FE-CP back card from an active RPM might cause an RPM failover.

- CSCeb44924

  When an MGX-RPM-1FE-CP back card is inserted, the “interface resets” field indicates an extremely large number of resets.

- CSCeb67443

  When a MGX-RPM-1FE-CP back card is replaced, the FE interface becomes active even though the interface is in a “shutdown” state prior to removing the back card.

- CSCeb69791

  The RPM hangs when trying to boot an IOS image from bootflash.

- CSCeb87633

  When an MGX-RPM-1FE-CP on an active RPM is removed (OIR), the RPM fails over as expected, but the other active RPMs in the redundancy group do not get marked as “blocked.”
- CSCec03589

  Packets are received out of order at their destination.
- CSCin35201

  The resolution of this enhancement caveat ports the latest relevant features and caveat fixes of the ATM_DELUXE_G10 firmware code (G124-G144) to the latest version of the RPM_ATMDELUXE_G10 ucode (G134).

Resolved Hardware Caveats

The following hardware caveat has been resolved at the time of the Cisco IOS Release 12.2(15)MC1 software release:

- CSCeb37123

  RPM-PR resetting without any crashinfo files being written or messages which indicate the cause of failure being logged in the PXM log or syslog.

Troubleshooting

This section contains the following MGX-RPM-1FE-CP troubleshooting information:

- Collecting Data for Back Card and Router Issues, page 12
- Modifying the MLP Reorder Buffer, page 12

Collecting Data for Back Card and Router Issues

To collect data for reporting back card and router issues, issue the following commands:

- **show tech-support**—Displays general information about the router when it reports a problem.
- **show logging**—Displays information in the syslog history table.

Modifying the MLP Reorder Buffer

When PPP multiplexing is disabled on the inbound direction of a MWR 1941-DC multilink, there are many more packets to reorder. Therefore, we recommend that you modify the MLP reorder buffer using the **ppp multilink slippage** interface configuration commands to avoid discarded fragments due to buffer overflow.

Slippage is the amount by which data arriving on one link in a multilink bundle might lag behind data transmitted over another link in that bundle. The amount of slippage might be expressed as a direct byte count, but it is also commonly expressed as a measure of time, in terms of the differential delay between the links.

A small amount of slippage between links is normal. Whenever slippage occurs, the multilink input process must buffer fragment data arriving on the faster channels until it receives all expected fragments on the remaining links, so that it can sort the fragments back into proper order, reassemble datagrams as necessary, and then deliver the datagrams in proper order to the higher network layers (multilink fragments include sequence numbers so that the multilink receiver can readily detect when packets are arriving out of order). The receiver must be capable of buffering enough data to compensate for normal slippage between the links, otherwise it will be incapable of completely sequencing and reassembling datagrams, and some data will be lost.

With Cisco IOS Release 12.2(15)MC1 and later, the MLP reorder buffer can be adjusted for cases where the slippage is larger than the defaults readily accommodate. The buffer size is set by defining a one or more constraints, each of which indirectly implies some byte limit. The limit used is the maximum of the value derived from the constraints.

To define the constraints that set the MLP reorder buffer size, issue the following commands while in interface configuration mode:

	Command	Purpose
Step 6	`Router(config-if)#` **`ppp multilink slippage mru`** *`value`*	Specifies that the buffer limit is *x* bytes where the byte count is expressed as a multiple of the maximum receive unit (MRU) negotiated for the bundle (the buffer limit is derived as the number of times defined for the *value* times the size of the largest packet received). Valid values are 2 through 32. The default is 8. **Note** The MRU is dynamically negotiated with the peer when the connection is established, therefore, the byte count also
Step 7	`Router(config-if)#` **`ppp multilink slippage msec`** *`value`*	Specifies the buffer limit, in milliseconds worth of data. Valid range is 1 to 16000. **Note** The actual amount of data buffered depends upon the bandwidth of the links.

Usage Notes

Note that these limits are on a "per-link" basis. For example, issuing **ppp multilink slippage mru 4** means that the total amount of data which is buffered by the bundle is 4 times the MRU times the number of links in the bundle.

The reassembly engine is also affected by the lost fragment timeout, which is configured using the **ppp timeout multilink lost-fragment** command.

The buffer limit derived from the slippage constraints implies a corresponding tolerated differential delay between the links. Since it does not make sense to be declaring a fragment lost due to a timeout when it is within the delay window defined by the slippage, the timeout will be dynamically increased as necessary so that it is never smaller than the delay value derived from the slippage parameters.

Documentation Updates

This section contains information that was not included or was documented incorrectly in the *MGX-RPM-1FE-CP Back Card Installation and Configuration Note*. 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 is documented as 150 per T1 interface and up to 600 connections per MLP bundle when in fact, 1000 connections are supported per MLP bundle regardless of whether the bundle contains one T1 interface or four.

The show ppp mux Command

The efficiency improvement factor calculation documented in the **show ppp mux** command section is incorrect. The correct improvement factor calculation uses bytes, not packets, and is as follows:

Multiplex efficiency improvement factor = 100 * (Total bytes saved) / (Total bytes received)

Where total bytes saved = bytes_received_at_muxer - bytes_sent_at_muxer.

Demultiplex efficiency improvement factor = 100 * (Total bytes saved) / (Total bytes sent)

Where total bytes saved = bytes_sent_at_demuxer - bytes_received_at_demuxer.

The show ip rtp header-compression Command

The **detail** keyword is not supported in the **show ip rtp header-compression** command on the MGX-RPM-1FE-CP back card. Output does not display for the `detail` keyword if specified in command.

Related Documentation

The following sections describe the available documentation related to the Cisco MGX-RPM-1FE-CP back card.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 in printed or electronic form.

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:

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

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.