Release Notes for Cisco MGX-RPM-1FE-CP Back Card for Cisco IOS Release 12.2(15)MC2e

November 2, 2005

Cisco IOS Release 12.2(15)MC2e

OL-2920-10

These release notes are for the Cisco MGX-RPM-1FE-CP for Cisco IOS Release 12.2(15)MC2e. 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)MC2e see the "Caveats in Cisco IOS Release 12.2(15)MC2e" section on page 9. To review the release notes for Cisco IOS Release 12.2, go to 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

Copyright © 2005. Cisco Systems, Inc. All rights reserved.

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 (maximum four per MLP bundle). The maximum throughput limit of RPM-PR with 1FE-CP is 120,000 packets bi-directional. In a 16 MLP interface case, the T1s are expected to be lightly loaded. 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.

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(15)MC2a, 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/en/US/products/hw/routers/tsd_products_support_category_home.html

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco MGX-RPM-1FE-CP for Cisco IOS Release 12.2(15)MC software.

New Features in the Cisco IOS Release 12.2(15)MC2e Software

No features are introduced in Cisco IOS Release 12.2(15)MC2e.

New Features in the Cisco IOS Release 12.2(15)MC2b Software

No features are introduced in Cisco IOS Release 12.2(15)MC2b.

New Features in the Cisco IOS Release 12.2(15)MC2a Software

No features are introduced in Cisco IOS Release 12.2(15)MC2a.

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

The following features were 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 7
- 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 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 12.2(8)MC2c, IP ID checking was suppressed in RTP/UDP header compression. With Cisco IOS Release 12.2(15)MC1 and later, a new option was 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, ACFC and PFC 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`	Re-enables 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`	Re-enables 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:

- Fast Ethernet 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)MC2e

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)MC2e. 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)MC2a. 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 DVD.

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

There are no known open caveats in Cisco IOS Release 12.2(15)MC2e.

Resolved Caveats

This section lists the caveats that are resolved in Release 12.2(15)MC2e.

- CSCea64571

  Description: The PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) sessions that go down may cause a leak of full virtual-access interfaces. This symptom is not observed with configurations that use virtual-access subinterfaces.

  This symptom is observed with PPPoE or PPPoA sessions that clear because of the PPP protocol goes down (because of a termination request [TERMREQ] from a peer router or a PPP **keepalive** failure). The leaked virtual-access interfaces are not reused for new sessions. This results in the creation of new virtual-access interfaces for new sessions.

  Workaround: There is currently no workaround.

- CSCea64843

  Description: A crash may occur when bringing up a large number of PPP over ATM (PPPoA) sessions.

  This symptom is observed on a Cisco router that is running Cisco IOS Releases 12.2(15)B and 12.3.

  Workaround: There is currently no workaround.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

Caveats in Cisco IOS Release 12.2(15)MC2b

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)MC2b. 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)MC2a. 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 DVD.

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

There are no known open caveats in Cisco IOS Release 12.2(15)MC2b.

Resolved Caveats

This section lists the caveats that are resolved in Release 12.2(15)MC2b.

- CSCec86420

  Description: Cisco routers running Cisco IOS supporting Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attacks on the MPLS disabled interfaces.

  This vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  This bug is a complementary fix to CSCeb56909 which addresses this vulnerability.

  More details can be found in the security advisory which is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml

- CSCed85438

  Description: A Fast Ethernet 100BASE-TX port adapter on an RPM-PR may stop receiving burst traffic packets.

  This symptom is observed on a FE RPM-PR Backcard. To identify this problem, the output of the **show interface fastethernet** command shows no input packets and all packets as overrun:

  30 second input rate 0 bits/sec, 0 packets/sec

  30 second output rate 100000 bits/sec, 106 packets/sec

  0 packets input, 0 bytes

  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

  0 input errors, 0 CRC, 0 frame, 263523 overrun, 0 ignored

  The output of the **show controllers** command for the Fast Ethernet interface shows high numbers for “rx_fifo_overflow” and “throttled”:

  throttled=5352, enabled=5352, disabled=0

  rx_fifo_overflow=434500, rx_no_enp=0, rx_state=0

  Workaround: To clear the symptom, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Fast Ethernet interface.

Further Problem Description: In the output of the **show controllers** command for the Fast Ethernet interface, locate the value for CFRV. If the last byte is either 0x20, 0x21, 0x22, or 0x23, the Fast Ethernet is susceptible to the symptom.

- CSCsa81379

  Description: NetFlow Feature Acceleration CLI.

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  This removal does not require an upgrade of your existing installation.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

cnfFeatureAcceleration	1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable	1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot	1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot	1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable	1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry	1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType	1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot	1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive	1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges	1.3.6.1.4.1.9.9.99999.1.3.4.1.6

Caveats in Cisco IOS Release 12.2(15)MC2a

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)MC2a. 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)MC2a. 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 DVD.

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 following caveat is open in Cisco IOS Release 12.2(15)MC2a.

- CSCeb24086

  Description: 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.

- CSCeb76514

  Description: 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 Cisco IOS 12.2(15)MC1.

Resolved Caveats

This section lists the caveats resolved in Cisco IOS Release 12.2(15)MC2a.

- CSCdz32659

  Description: Memory allocation failure (MALLOCFAIL) messages no longer occur for Cisco Discovery Protocol (CDP) processes.

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

- CSCec21937

  Description: When the MGX-RPM-1FE-CP FastEthernet interface is administratively shut down, for directly connected devices, the interface still appears to be up.

- CSCec25430

  Description: A Cisco device reloads on receipt of a corrupt CDP packet.

- CSCed40563

  Description: Problems with the CDP protocol have been resolved.

- CSCin67568

  Description: A Cisco device experiences a memory leak in the CDP process. The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Troubleshooting

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

- Collecting Data for Back Card and Router Issues, page 14
- Modifying the MLP Reorder Buffer, page 14

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 Documentation: Cisco IOS Software: Cisco IOS Release 12.2: New Feature Documentation:12.2-Based New Features: New Features in Release 12.2 MC

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.htm

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Release Notes for Cisco MGX-RPM-1FE-CP Back Card for Cisco IOS Release 12.2(15)MC2e

© 2005, Cisco Systems, Inc All rights reserved.