Release Notes for Cisco MGX Route Processor Module (RPM-XF) IOS Release 12.3(7)T3 for PXM45-based Switches, Release 5.0.10

These release notes are part OL-6305-01 Rev. A0, August 18, 2004

Contents

About These Release Notes 3
Special Notes 3
New Features 3
Features Introduced with 12.3(7)T3 4
Features Introduced with 12.3(2)T6 5
Features Introduced with 12.3(2)T5 5
Features Introduced with 12.3(2)T4 5
Link Fragmentation Interleaving (LFI) 5
Increase the Maximum Number of Policy Maps to 2048 5
MPLS VPN Multicast 5
cRTP 6
WRED Drop Counters 6
TMS 6
SAR based TM/QoS 6
TCP de-compression 6
Dual MPLS Partition for RPM-XF (related to LSC redundancy) 6
Feature Introduced with 12.3(2)T2 7
2-Port POS (Packet Over SONET) and 2-Port GIG-E (Gigabit Ethernet) Service Module Back Cards 7

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

Copyright © 2002, 2003. Cisco Systems, Inc. All rights reserved.

Features Introduced Prior to 12.3(2)T2 7
MGX 8950 Support for RPM-XF 7
EiBGP Load Balancing 7
IP Accounting Counters 8
Multiple Actions under Police Command 9
QoS Sub Optimal Link Utilization 9
RPM-XF Redundancy Support 10
Features Not Supported in This Release 10
Network Management Features 11
SNMP MIB 11
RPM-XF Limitations and Restrictions 11
Notes and Cautions 13
RPM-XF auto_config File Management 14
Card Management 14
RPM-XF Bootflash Precautions 15
Solving the RPM-XF Bandwidth Issue When Adding a 12th VISM Card 15
Open Anomalies —Release 12.3(7)T3 for RPM-XF 16
Resolved Caveats—Release 12.3(7)T3 18
Resolved Caveats—Release 12.3(2)T6 19
Resolved Caveats—Release 12.3(2)T5 21
Resolved Caveats—Release 12.3(2)T4 21
Resolved Caveats—Release 12.3(2)T2 23
Compatibility Notes 25
RPM-XF Boot File and Firmware File Names and Sizes 25
RPM-XF Compatibility Matrix 25
MGX RPM-XF Hardware 25
Cisco IOS Release Compatibility Information 26
Using XModem to Download Flash to RPM-XF Cards 26
Historical Information for 12.2.x IOS Baseline 28
Resolved Caveats—Release 12.2(15)T5 28
Resolved Caveats in Release 12.2.15T 30
Resolved Caveats Prior to Release 12.2.15T 33
Related Documentation 47
Obtaining Documentation 47
Obtaining Technical Assistance 48
Obtaining Additional Publications and Information 49

About These Release Notes

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

Note that for Release 5.0.10 user documentation (command reference, overview, and installation and configuration guides), use the MGX Release 5 and Cisco IOS documents in addition to this release note.

Product documentation for Release 5 of the MGX 8850 is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/rel5/index.htm

Product documentation for Release 5 of the MGX 8950 is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8950/rel5/index.htm

Special Notes

Please refer to the this Web page for the latest updates on IOS software and firmware issues.

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/printsa.pl?get_crypto=&data_from=&hardware_name=&software_name=&release_name=12.3.2T&majorRel=12.3&state=:RL&type=Early%20Deployment&file=12.3.2T.c.html

Note that the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4* manual describes some features that are not supported in this release. Refer to the section entitled "Features Not Supported in This Release" section on page 10 for a list of the affected features.

New Features

The MGX RPM-XF is a next-generation, high performance model of the RPM for the MGX 8850 and MGX 8950 platforms, using PXM45 processor modules. It is a router module based on an RM7000A MIPS processing engine that fits into slots 1-6 and slots 9-16 in the MGX 8850 and slots 1-6 and slots 11-16 in the MGX 8950.

The RPM-XF hardware provides forwarding technology for packet switching capabilities in excess of 2-million pps. The forwarding engine is packet based and is interfaced to the midplane of the system through a combination of switch interface technologies. For more information on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

Features Introduced with 12.3(7)T3

The following new features were introduced with release 12.3(7)T3:

- MGX-XF-UI/B notched backcard

  The MGX-XF-UI/B notched back card is a re-spin of the user interface back card for the RPM-XF. The notch has been added to allow clearance for installation of the RCON APS connector on the Cisco MGX 8850B and MGX 8880 chassis.

- Preferred Routes on RPM-XF

  IOS software release 12.3(7)T3 introduces enhanced support for preferred routes on the RPM-XF. Currently the AXSM and other service modules provide the facility to "associate" an already defined preferred route on the PXM to an SPVC mastered on that service module. The following commands have been updated to support Preferred Route association via CLI or SNMP for SPVC/Hybrid/XPVC connections that have an RPM-XF as the master end:

Syntax Description

Router(config-if-swconn)#[no] prefrte <Route ID>

The Route ID is an identifier for the configured preferred route that is being associated with this connection. Preferred routes are manitained in a separate database on the PXM and referenced by the ID. The range is 0 through 65535. Setting the ID to 0 means no preferred route is configured. The default value for preferred route ID is zero (no preferred route attached).

Router(config-if-swconn)#[no] directrte

Setting the Directed Route flag to Yes means that the user wants the connection to be routed only on the specified preferred route. "The default value for directed route is No.

Router(config-if-swconn)# prefrte ?

<1 - 65535>Preferred Route ID value

Router(config-if-swconn)# directrte ?

<cr>

Note If you try to use the directrte command to specify a directed route for a connection with its preferred route ID set to zero, an error message displays. Both the prefrte and directrte commands must be run on the master end of the connection. If you try to use these commands on the slave end of the connection, an error message displays.

Examples

To configure a preferred route ID value of 10 for the connection.

```
Router(config-if-swconn)# prefrte 10
```

To configure a preferred route id value of 5 AND set the connection on directed route-

```
Router(config-if-swconn)# prefrte 5
Router(config-if-swconn)# directrte
```

To change the directed route flag for the connection to NO-

```
Router(config-if-swconn)# no directrte
```

To set the preferred route id to zero AND set the directed route to NO-

```
Router(config-if-swconn)# no prefrte
```

Features Introduced with 12.3(2)T6

The following new features were introduced with release 12.3(2)T6:

- eiGRP between CE to PE
- Basic PPP over ATM feature evaluation on various port speeds from 768Kbps up to DS3 with a maximum of T1 bandwidth per flow.
- PPP over ATM with cRTP on various port speeds from 768Kbps up to DS3 with a maximum of T1 bandwidth per flow.
- PPP over ATM with cRTP and QoS enabled on the links.
- Scaling up to 200 cRTP enabled pppoATM links with QoS

Features Introduced with 12.3(2)T5

No new features were introduced with release 12.3(2)T5.

Features Introduced with 12.3(2)T4

Link Fragmentation Interleaving (LFI)

The 12.3(2)T4 release adds support for Link Fragmentation Interleaving (LFI). For more information on the CLI commands that have been introduced or modified to support this feature on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

IOS configuration information can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtlfifra.htm

Increase the Maximum Number of Policy Maps to 2048

Policy maps along with class maps and service policy maps are used to define a traffic policy and attach them to an interfaces. Prior to this release, you were able to create 256 separate policy maps and a total of 256 class maps per policy map. With this release, the maximum number of policy maps has been increased to 2048. Each policy map supports up to 32 class maps per policy map. For more information on the CLI commands that have been introduced or modified to support this feature on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

MPLS VPN Multicast

The frame-based Multicast VPN (MVPN) feature enables the RPM-XF to pass frame-based multicast traffic to VPNs across the ATM core.

Configuration information can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_mvpn.htm

cRTP

The cRTP acronym refers to the Compressed Real-Time Protocol (CRTP) header. This release of the RPM-XF adds the ability to configure this header.

Below are the CLI commands introduced to support this feature:

- ip rtp header-compression - enables RTP header compression for a particular interface.
- no ip rtp header-compression - disables RTP header compression for a particular interface.
- clear ip rtp header-compression <interface> - resets all statistics for the interface to 0.
- show ip rtp header-compression <interface> [detail] - shows all statistics for an interface.
- show policy-map int sw1.x -shows the number of packets which are compressed because of match in policy map.

Configuration information can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/fthdrcmp.htm

WRED Drop Counters

The WRED Drop Counters feature adds Class-Based Packet Counters to existing RPM-XF functionality. The counters can be dscp based or precedence based. For more information on the CLI commands that have been introduced or modified to support the WRED Drop Counters feature on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

TMS

The TMS (Traffic Matrix Statistics) feature allows an administrator to gather the number of packets and bytes that travel across the backbone from internal and external sources. These packets and bytes are called traffic matrix statistics. Use the statistics collected to determine how much traffic the backbone handles. The statistics are always collected on the incoming interface. For more information on the CLI commands that have been introduced or modified to support TMS on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

SAR based TM/QoS

Traffic Management, Weighted RED, and Cell-Based Weighted Fair Queuing algorithm processing is now accomplished using the Segmentation and Reassembly engine (SAR).

TCP de-compression

The 12.3(2)T2 release adds support for TCP de-compression as an adjunct to supporting the Compressed Real-Time Protocol (CRTP) header feature on the RPM-XF.

Dual MPLS Partition for RPM-XF (related to LSC redundancy)

The 12.3(2)T2 release adds support for dual MPLS partitions on the RPM-XF.

Configuration information can be found at
http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px1e/rel4/scg/rpm.htm

Feature Introduced with 12.3(2)T2

2-Port POS (Packet Over SONET) and 2-Port GIG-E (Gigabit Ethernet) Service Module Back Cards

The 12.3(2)T2 release adds support for two new service module back cards that provide either two GIG-E (Gigabit Ethernet) or two POS (Packet Over SONET) ports. For more information on the fit and function of these 2 new service module back cards as well as the CLI commands that have been introduced or modified to support these 2 new service module back cards on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4.*

Features Introduced Prior to 12.3(2)T2

MGX 8950 Support for RPM-XF

In Cisco MGX Release 3.0.10 and later, the MGX 8950 supports the MGX RPM-XF card set. The MGX RPM-XF card set can occupy any of the available service module slots in the MGX 8950, which are slots 1-6 and slots 11-16.

EiBGP Load Balancing

To balance load by BGP on multiple paths to destination, traffic is directed on multiple available paths between autonomous systems (AS) by gateway routers.

The following CLI commands are used to implement this feature.

Command	Description

maximum-path <*nums*>	Configure maximum number of EiBGP parallel routes.
	For example:
	`bgpbox-zenith-CE1(config)#router bgp 4`
	`bgpbox-zenith-CE1(config-rout)#maximum-paths 3`
	`bgpbox-zenith-CE1(config-rout)#end`

show ip bgp	This command has been enhanced to show the multipaths.
	Each multipath is marked as 'multipath'.
	The bestpath is marked as 'multipath' and 'bestpath'.
	The output also has what flavour of multipath is enabled.
	For example:
	`bgpbox-zenith-CE1#sh ip bgp 141.22.0.0`
	`BGP routing table entry for 141.22.0.0/16, version 18`
	`Paths: (2 available, best #1)`
	`Multipath: eBGP`
	`Advertised to non peer-group peers:`
	`7.0.76.9`
	`100 5`
	`7.0.76.2 from 7.0.76.2 (100.0.0.2)`
	`Origin IGP, localpref 100, valid, external, multipath, best`
	`100 5`
	`7.0.76.9 from 7.0.76.9 (100.0.0.9)`
	`Origin IGP, localpref 100, valid, external, multipath`

Limitations:

- If there are multiple alternate paths for the peering point, only one of the paths is utilized for a given prefix.
- Only per-flow load balancing is supported. Per-packet load balancing is not supported.
- Supported only in MPLS/VPN networks.
- Load balancing proportional to the link's bandwidth [dmz-linkbw] is not supported. The load balancing will be performed on the available links with equal costs.
- The maximum number of paths that can be used for load sharing is 6. This is the current IOS limitation too.
- Load balance will not work if RDs are same with RR. RDs have to be different if RRs are used.
- CEs in different VPNs using same RDs does not work.

IP Accounting Counters

MGX RPM-XF stores the packet/byte counters based on precedence/DSCP values on a per interface level at input ONLY.

The following CLI have been added or enhanced for this release to implement this feature:

Command	Description
ip accounting ?	pop20-slot6(config-if)#**ip accounting ?** precedence Count packets by IP precedence on this interface dscp Count packets by DSCP on this interface
ip accounting precedence ?	pop20-slot6(config-if)#**ip accounting precedence ?** input received packets and bytes
ip accounting dscp ?	pop20-slot6(config-if)#**ip accounting dscp ?** input received packets and bytes
show int [interface] precedence	pop20-slot5# **show int [interface] precedence**
show int [interface] dscp	pop20-slot5# **show int [interface] dscp**
clear counters	pop20-slot5#**clear counters**

Limitations:

- Counters are maintained ONLY at input per interface.
- There is no count of dropped/transmitted based onDSCP/PREC packets per interface.

Multiple Actions under Police Command

The MGX RPM-XF **police** command is now similar to the IOS/RPM command. Therefore, multiple **exceed** and **conform** actions can be applied on the **police** command.

The **police** CLI command has been enhanced as follows:

Prior to this release, the **police** command had no menus and all parameters were listed on one line, as shown in the following example.

```
domino80p01-z001#sh policy test1z
    ..............
    police 128000 8000 8000 conform-action transmit exceed-action drop
```

This allows only one value for *conform-action* and *exceed-action*.

The newly enhanced **police** command functions as shown in the following example.

```
ipfrtx90r14-01(config-pmap-c)#police 128000 8000 8000
ipfrtx9(config-pmap-c-police)#conform-action transmit
ipfrtx9(config-pmap-c-police)#exceed-action set-dscp 28
ipfrtx9(config-pmap-c-police)#exceed-action set-mpls 2
```

Note that multiple **conform-action** and **exceed-action** parameters can be configured.

QoS Sub Optimal Link Utilization

RPM-XF uses VTMS as a scheduling algorithm. VTMS schedules queues based on the current link utilization in real time. The previous version of the VTMS algorithm was efficient and mapped well in an ASIC or network processor. However, it did not fully utilize the link.

In this release, a fix is made (via a new CLI command) to allow the user to specify the over subscription factor on a queue. The factor is in the range on 1-31 and can be denoted as 2n. An over subscription factor of n = 2 on any queue, essentially means to subscribe that queue by a factor of 4 (2n where n (in this example) is 2; so 2 raised to power 2=4).

The new syntax for bandwidth and priority commands are:

```
[no] bandwidth {<kbps> | percent <percentage> | remaining percent <percentage>}
[maximize-utilization [<max-shift>]]

[no] priority {<kbps> | percent <percentage>} [maximize-utilization
```

RPM-XF Redundancy Support

RPM-XF 1:N redundancy is used to switch configuration and traffic from one RPM-XF module to another RPM-XF module. Route processing continues with minimal traffic loss even if an RPM-XF fails and there is no operator or direct access to swap the failed card or fix the problem. Currently we support redundancy that ensures Layer 2 state restoration. Layer 3 state is restored via convergence.

Note When resetting a shelf with RPM-XFs configured for 1:N redundancy, it is recommended that you bring up the primary slots in active state.

The main benefits of 1:N Redundancy are:

- An RPM-XF card with hardware problems can be fixed while the redundant standby card takes over its functionality.
- Software upgrades are easier and can be done with less downtime.
- LAN interface redundancy supported with MAC addresses of primary RPM-XF copied to standby RPM-XF.
- 1:N Redundancy support for Gigabit Ethernet interface backcards during front card switchover.
- Y cable redundancy support for POS backcards during front card switchover. (With Y cable, 1:N redundancy is restricted to N = 1).

The following are the general guidelines for redundancy on the RPM--XF:

- **Addred** is not allowed between RPM-PR and RPM-XF.
- To configure redundancy, the Primary RPM-XF should be in Active state and Secondary RPM-XF card must be in Active/Standby state.
- Removal of the Active RPM-XF back card does not cause switchover to the standby RPM-XF.
- User has to make sure that **E:RPM/auto_config_slot#** is created before adding redundancy. This may require a login to primary card through the command line and manually adding **boot config e:auto_config_slot#** followed by a **write mem**.
- Executing **switchcc** back-to-back with **switchredcd** can cause problems. We recommend giving a gap of at least 5 seconds between **switchredcd** and a **switchcc**.
- IOS software on a standby card should be the same or higher version than the Active RPM-XF card.
- Booting the card from an image on tftp server is not recommended when the card is in redundancy group. The card should be booted from image in bootflash or PXM disk only.
- Configuring the standby RPM-XF is not recommended.

Features Not Supported in This Release

The following features are not supported in this release.

- LSC Redundancy
- MPLS TE tunnels on ATM Interfaces
- VC Merge
- RPM-PR to RPM-XF upgrade
- OIR of backcards without interfaces in shutdown mode
- Per packet load balancing
- Modem connectivity on Auxiliary port
- ROMMON's Xmodem functionality does not support the Speed option.

Network Management Features

Network management features are detailed in the *Release Notes for Cisco WAN Manager 15.0.00* at:

http://cisco.com/univercd/cc/td/doc/product/wanbu/svplus/15/rnotes/index.htm

SNMP MIB

SNMP MGX Release 5.0.00 MIB files are provided with the delivery of this release. The MIB files are in standard ASN.1 format and are located in the same directory within the release bundle on CCO. These files may be compiled with most standards-based MIB compilers. The tar file for MIB contains the file that contains the MIB release notes. This contains only MGX MIBs.

Cisco IOS MIBs are not part of this bundle. They are part of the 12.3(2)T6 CCO release.

RPM-XF Limitations and Restrictions

The RPM-XF limitations and restrictions that apply to this release are as follows:

- **E: RPM/auto_config_slot#** must be created before adding redundancy. This may require a login through the CLI and manually adding the **boot config** command followed by a **write mem**.
- PVPs can not operate at a rate greater than 599039 kbps.
- High speed VC (SCR greater than or equal to 599,039 kbps) would not get full-configured rate for single flow (unique source and destination IP address). This happens because for high speed VCs, the PXF creates two queues and these queues can't be shared for same stream. Sharing two queues for same stream would cause out of sequence packets.
- PXF queue selection algorithm may cause traffic drop for multiple stream going to same destination via multiple paths. When the PXF gets a packet, it selects the output queue based on source and destination IP address. These addresses hash into one of the queues for the selected destination. So if there are multiple paths for the same destination, there is a possibility that multiple streams would hash to one queue, causing some queues to overflow, while others might be under-utilized.
- PXF buffer depletion may occur if packets of the same size (especially packets greater than 640 bytes) are sent to a congested interface.
- Currently VBR-nrt and VBR-rt are treated with same priority system wide.
- RPM-XF PVP only supports UBR.

- PVP in RPM-XF is not OAM managed.
- If out-of-sync SPVC or SPVP exist on RPM-XF, shrinking of PNNI partition would not be permitted.
- A single RPM-XF can only function as either an Edge LSR or as an LSC, but not as both.
- Because RPM-XF only supports UBR, VBR-rt and VBR-nrt, on the PXM, **dsppnportrsrc** for RPM-XF port will show 0 available resource for CBR, ABR and signaling service types. Also, **cnfpnportcac** for CBR and ABR will be rejected.
- If RPM-XF is configured as an eLSR, RPM-XF does not support incoming VC-merge LVCs. There is a problem logged against LSC module that it cannot support both VC-merge/non-VC-merge supporting VSI slaves at the same time. So for now, if RPM-XF eLSR is part of a cell based MPLS network (with RPM-PRs or AXSMs in the same node), disable the VC-merge feature on LSC. (Note that VC-merge is enabled on LSC by default).
- RPM-XF eLSR only supports at most two MPLS sub-interfaces. Attempting to configure over the limit will result in an error message.
- Although RPM-XF VSI slave supports connections statistics Get command, only packets and bytes counts are available. Therefore, **show xtag cross-connect traffic int xtagatm** connection statistic display on LSC are actually packet counts from RPM-XF eLSR.
- OIR of MGX-1GE and MGX-1OC12POS-IR back cards are supported only with interfaces in *shutdown* state.
- MGX-1GE back card does not have the capability to provide line loopback.
- Flow Control Option is not configurable with MGX-1GE back card.
- MGX-1GE back card does not support SFP security.
- Line loopback and internal loopback cannot be set at the same time for the MGX-1OC12POS-IR back card with AMCC Mux.
- **pos ais-shut** command is not supported on MGX-1OC12POS-IR back card.
- Traffic rate per flow is at half the interface speed for POS/GigE interfaces in this new release.
- Autonegotiation is not recommended to be toggled on GigE interfaces when traffic is going through. This may result in permanent disruption of traffic.
- For UBR 2 queues always exist which would result in half the Flow rate for each flow because of hashing algorithm hashing into single queue .

The performance limits supported in this release are the following:

- 2K ATM SPVC Connection endpoints
- 2K IDBs
- 4K LVCs
- 100 VPCs
- 256 Policymap
- 100 OSPF neighbors
- 6 IOS-based cards in MGX shelf
- 500 VRFs: 500
- 500 BGP CE Peers
- 100 RIP CE sessions
- 500 Static CEs

- 100,000 VPN Routes per PE
- 250K non-VPN Routes per RPM-XF
- 50 Xtag interfaces per RPM-XF
- 300 OAM enabled connections

For more RPM-XF performance details, contact your sales representative.

Notes and Cautions

The following notes and cautions should be reviewed before using this release.

- Attempting to initiate RPM-XF switchover when **write mem** is in progress on the active RPM-XF card may lead to the card coming up with a partial configuration. When an **addred** is executed, an automatic **write mem** is triggered on the primary RPM-XF. If the primary card fails when the **write mem** is in progress, the card may come up with a partial configuration. The duration of **write mem** depends on the configuration size and can take up to 4 minutes to complete.
- There is a new stable “Boot-Hold” state displayed on the PXM45 when **dspcds** is executed. This state indicates that the RPM-XF is running only boot image. This state is reached when config register is set to 0x1 or when the bootldr cannot find the run-time image, but found the boot image. Enter **cc** to access the RPM-XF from the PXM45.
- Valid boot image need not be the first file in the boot flash. The RPM-XF will load from any valid boot image from the **bootflash:**. The run-time image can be the first file in the boot flash and RPM-XF will come up with that image.
- Trying to change PCR value of VP tunnel or changing MTU of switch interface with more than 4K VCs may cause CPU hog.
- If there is a large number of VCs (PVCs or LVCs or both) on RPM-XF card, executing disruptive operations on the main switch interface (int switch1) may cause flapping of protocols that run on these VCs. Examples of disruptive operations are **clear int switch1** and modification of PVP parameters. These operations cause deactivation and re-activation of all VCs under the main switch interface. Depending on the number of VCs, the time required to complete such operations may exceed certain protocol timeout limit. Examples of protocols that may be affected are OSPF and TDP/LDP.
- RPM-XF VSI slave tends to output informational warning/trace back messages caused by misconfigurations and CAC failures (onto console/IOS log file). These messages are mostly for information/debugging purpose. When these messages are observed, confirm that connection status is still intact and traffic is still passing successfully.
- Due to PXF scr granularity, the configured scr on IOS *pvc* CLI may not be the same as the actual scr programmed in the PXF. PXF bandwidth chunk size is 18 kbps; all PXF VC scr will be programmed as multiples of 18 kbps. For instance, if the PVCs were configured with 50 kbps as pcr, 54 kbps would be programmed in PXF. **show atm pvc** display will show 50 kbps, and VSI Slave will account 50 kbps during CAC. However, 54 kbps is actually being used. So as a result, when bandwidth usage is reaching the maximum value, both VSI Slave and PNNI will continue to allow connection provisioning, because VSI Slave and PNNI available bandwidth shows more than PXF actually has left.
- **Saveallcnf** (issued on the PXM45/B card) captures configuration data saved by the RPM-XF card (as well as AXSM and PXM45 cards), and saves it on the active PXM45/B card’s hard disk. Configure the RPM-XF to store its configuration on the PXM45/B hard disk (E:/RPM) by entering **boot config e:auto_config_slot#** in the running configuration of the RPM-XF. To ensure that the saved file contains

the latest RPM-XF configuration, execute the **write mem** command on each RPM-XF card prior to the entering **saveallcnf** command. This also ensures that the RPM-XF files on the active PXM45 hard disk will contain the latest configuration to be saved.

- For ELSR to LSC connectivity, the default control VC used is 32. If PNNI partition exists with VCI 32 as part of its partition range, when an MPLS partition is added, there are two options to handle the situation:
  - Add the MPLS controller and define its partition with available range. On eLSR, define control VC from any VCI value within the range defined in partition. The same VC should be defined on LSC on xTag interface.
  - Reconfigure PNNI partition to spare the control VC usage both on RPM-XF and AXSM, AXSM/B or AXSM-E APS Management Information.
- Whenever the RPM-XF configuration is changed, enter the **write mem** command on the RPM-XF to save the configuration. If this is not done, the changed configuration will be lost on an RPM-XF card reboot or RPM-XF switchover, in the case of redundancy.

RPM-XF auto_config File Management

The RPM-XF *auto_config_slot#* file stores the configuration for the RPM-XF card. The *slot#* portion of the name should be set to the logical slot number that corresponds to the RPM-XF card. This file can be stored in bootflash or in the E:RPM directory on the PXM45 hard disk. The configuration is also stored in NVRAM using the name startup-config.

When the RPM-XF card is inserted or rebooted, it searches for the configuration file in the following sequence:

1. If there is an auto_config file corresponding to its logical slot on the PXM45 hard disk, the RPM-XF card uses the configuration stored on the hard disk.
2. If boot variable points to configuration stored in the PXM45 hard disk or Bootflash and if the file is not found, the card comes up as Active-F with the default configuration.
3. If there is no auto_config file on the hard disk, then the NVRAM version is used.

Note In case of RPM-XF redundancy, the configuration should always be stored in *auto_config_slot#* file in the E:RPM directory of the PXM45 hard disk. Failure to find the auto_config file will lead to aborting of a user-initiated switchover (**switchredcd**) and a fatal error will be flagged.

Card Management

The following card management notes and cautions should be reviewed before using this release.

- There is a new stable state displayed on the PXM **dspcds** command—**Boot-Hold**, which signifies that the RPM-XF is running the boot image only. On the RPM-XF, the prompt will display as *boot>*
- The run-time IOS image cannot be used as a bootloader to load a different IOS image.
- Change of console speed on the terminal server may cause the card to end up in the ROMMON state. To avoid this, set the config register to **0**x2102.

  Another workaround is to enter **cont** on the ROMMON within 2 minutes of going into ROMMON state. This will bring the card to its original stable state.

Note It is recommended to always use 9600 baud as the console speed.

- The IOS version of the runtime as well as the boot image will be displayed in the **dspcd**, **dsprevs**, and **dsprevs -s** output. The version will be displayed under the heading of IOS version. Revision Control is not available for RPM-XF (like RPM-**PR).**

Note The commands **loadrev** and **setrev** do not apply for RPM-XF.

RPM-XF Bootflash Precautions

The RPM-XF bootflash is used to store boot image, configuration and *run- time* files. Erasing the boot image from the Flash will cause the card to not boot.

The RPM-XF boot image, which comes loaded on the Flash, will work for all RPM-XF IOS images. Therefore, there is no reason to delete or move the factory installed boot image.

In order to avoid any unnecessary failures that would require card servicing, do the following:

- Never erase the boot file from the RPM Flash
- Never change the position of the boot file on the RPM Flash
- Use care when “squeezing” the Flash to clean it up.

As long as the boot file remains intact in the first position on the flash, the RPM-XF will boot successfully.

If the bootflash is corrupted, use the **tftpdnld** procedure described in the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide* or xmodem procedure described in “Using XModem to Download Flash to RPM-XF Cards” later is this document to download a new boot image.

Solving the RPM-XF Bandwidth Issue When Adding a 12th VISM Card

Adding more than 11 VISM cards to an MGX chassis with RPM-XF cards requires enabling the expanded memory option on PXM45/B. The command to enable this option is cnfndparms (option 4). This expanded memory option does not impact chassis performance while allowing more connections.

Open Anomalies —Release 12.3(7)T3 for RPM-XF

Table 1 lists the open caveats in Cisco IOS Release 12.3(7)T3 as of August 18, 2004.

Table 1 Open Anomalies on 12.3(7)T3 for RPM-XF

Caveat Number	Description
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.
CSCed05924	Symptom: PXF reloaded abnormally due to software exception %PXF-2-FAULT:T0 SW Exception:CPU[t0r3c1] 0x00000180 at 0x0DE1 LR 0x084B Conditions: MVPN traffic was being passed. No other activity on the card at that time. Workaround: Unknown.
CSCed34575	Symptoms: MPLS packet will be transmitted without fragmentation even if the MPLS packet exceeds the outgoing interface MTU. Conditions: When the MPLS packet is greater than the outgoing interface MTU. Workaround: None.
CSCed39641	Symptoms: SAR rx drops all packets due to no buffer Conditions: RPM-XF configured as PE in frame-based or cell-based MPLS/VPN network. Execute “sh pxf cpu buff leaked 0-5” or “clear interface sw1” command while system is under load, may cause SAR rx failure. Workaround: None.

Table 1 Open Anomalies on 12.3(7)T3 for RPM-XF (continued)

Caveat Number	Description
CSCed48954	Symptoms: Traffic will tail drop on the output of GigabitEthernet interface even when the traffic rate is well below the interface limit. Condition: This problem seems to happen after multiple GigabitEthernet interface flaps. Workaround: Reload the PXF using “microcode reload pxf” command.
CSCed86771	Symptoms: Pull/insert RPM-XF while running call rate, made the card to reload/failed. Conditions: While running 360K BHCA (Busy Hour Call Attempts) with 120 sec CHT. Upon pulling one of RPM-XF card and putting it back into the rack, this RPM-XF card rebooted and went to failed state. Workaround: None.
CSCee36771	Symptoms: A PPPoA interface constantly flaps when passing data with SAR-based CBWFQ enabled. Conditions: This has been observed under the following conditions: - SAR-based CBWFQ is enabled on a PPPoA interface. - the class default is assigned a very small bandwidth (less than 10 percent) - all classes on the VC are congested. Workaround: Assign 10 percent bandwidth to the class-default of the policy map attached to the interface.
CSCee53246	Symptoms: The standby (secondary) Route processor Module does not release the config_file boot variable after the primary redundant RPM-PR card takes over after the card switch over command was executed. Conditions: This intermittent problem was observed after a switchover from secondary RPM-PR card to primary RPM-PR card. Secondary (redundant) card is in Standby state, but the “show bootvar” command still shows that config_file variable is not null. Workaround: Unknown.

Table 1 Open Anomalies on 12.3(7)T3 for RPM-XF (continued)

Caveat Number	Description
CSCee74057	RPM throughput performance degradation in pi5 branch
CSCea84387	Two simultaneous policy map displays cause problems Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive. Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions. Workaround: Allow only one user at a time to enter MQC commands.

Resolved Caveats—Release 12.3(7)T3

Table 2 lists the resolved caveats in Cisco IOS Release 12.3(7)T3 for MGX 5.0.10 as of August 18, 2004.

Table 2 Resolved Caveats in Cisco IOS Release 12.3(7)T3 for MGX 5.0.10

Caveat Number	Description
CSCee54524	During SCR provisioning (changing the bandwidth) on the ePVCs, the RPM-PR (Route Processor Module) PE may reload.
CSCed41381	LSNT: Input drops on framed PVC i/f cause ldp session flap
CSCed74835	When copying big files from Cisco MGX8850 Route Processor Module (RPM-PR) to MGX8850 hard drive, it silently failed.
CSCea85395	BGP suppressed prefixes not reinstated after condition removed
CSCea62571	%UTIL-3-TREE: Data structure error with trace back logged on LSC
CSCed41823	LSNT: Tx SAR stuck after micro rel sar tx/rx issued
CSCed74882	OSPF: CPUHOG Traceback on reload with large no of sec. ip addresses
CSCed88043	The outgoing VCCI programmed in the FIB/TFIB in the PXF for a prefix is wrong.
CSCed92418	back to back clear int sw1 causes VSI down on PXM
CSCee06261	LSNT: RP crash on rpmxf_is_atm_mlp_configured while clear int sw1
CSCee12415	Multicast traffic is not getting switched correctly.
CSCed16744	Traffic does not resume after SAR is brought out of hang state.
CSCee23320	Router might reload upon deletion/re-apply of policy-map.

Resolved Caveats—Release 12.3(2)T6

Table 3 lists the resolved caveats in Cisco IOS Release 12.3(2)T6 as of June 4, 2004.

Table 3 Resolved Caveats in Cisco IOS Release 12.3(2)T6

Caveat Number	Description
CSCdy81782	no shut on the ppp interface before VA goes down causes pxf to drop
CSCed46603	MIB walk on ifOutDiscards object OID returns an error message.
CSCed53155	After failure recovery, the SAR Segmenter is not programmed correctly.
CSCed62886	TagI counter always shows 0 in the output of “show pxf cpu cef mem” command.
CSCed68881	“sh controller” output is not part of sar info files.
CSCed71495	The exp bit on the topmost label is not changed when set mpls exp topmost is configured on the ingress interface of the P router.
CSCed75086	When issuing the command show pxf cpu rewrite verification x.x.x.x you receive an error message stating that the “Channel ID in the SAR header is non-zero (x) for MVC”
CSCed82673	An RPM-XF card may reload abnormally when issuing some of the display commands under “show rpm vsis core conn debug-command <WORD> <Argument#1>”
CSCed41381	Input cell drops may occur on an ingress frame PVC that is configured on a switch interface. This situation may cause LDP/TDP/OSPF flaps.
CSCed71750	Virtual-Access counters doesn't match the ATM subinterface counters.
CSCed91750	S,G entries are not being created in the core.
CSCee00031	The `average packet size' displayed under `show ip mroute count' doesn't exactly match the actual size of the multicast packet being sent.
CSCee00685	Wrong DSCP values set on IP packets.
CSCee02220	Multicast traffic flows use default MDT instead of data MDT for some VRFs.
CSCeb05118	A Cisco MGX Route Processor Module (RPM-XF) router that is configured as an Edge Label Switch Router (ELSR) may reload when deleting Multiprotocol Label Switching (MPLS) type subinterfaces.
CSCee40165	The “show policy interface multilink <int> output” command shows incorrect counts for the dscp value tabulation at the end of the command output when rtp header compression is enabled under the multilink interface.
CSCec21461	On the RPM-XF, the input packet count for Virtual-Access interfaces are higher than the actual number of packets received.
CSCed22425	On the Cisco RPM-XF router, there is no way to know which external Border Gateway Protocol (eBGP) path is chosen when there are multiple VRF interfaces to the VPN prefix.
CSCed41273	PXF gets reloaded abnormally several times after microcode reload.
CSCed42706	On the Cisco RPM-XF router, the PXF does not increment the correct drop code when dropping packets.

Table 3 Resolved Caveats in Cisco IOS Release 12.3(2)T6 (continued)

Caveat Number	Description
CSCed68717	Incoming traffic is not being forwarded.
CSCed70687	PXF buffer allocate failure happens on ELSR.
CSCed78131	Checksum errors are reported on cRTP traffic streams.
CSCed83738	Packets on cRTP-enabled PPPoA interfaces that match classes other than "class-default" will be dropped.
CSCed89382	On Multilink Protocol interfaces using Link Fragmentation and Interleaving, the Fragmented Pkts counter under the "show pxf cpu subblocks Multilink1" command, increments when it should not.
CSCed90333	Traffic is not forwarded through a newly added CBWFQ class.
CSCed94549	A compressed packet from XF is rejected by the RPM-PR as a CRC error.
CSCed96053	Does not show precedence ip accounting for rtp/udp compression packets.
CSCee00038	Protocols flap when the non-ATM (POS or GigE) interfaces are congested by high traffic.
CSCee02404	PXF buffer leak, loss of connectivity, BGP dn on the PE-CE VRF link with cRTP enabled.
CSCee03726	PXF buffers are leaked.
CSCee07654	Starting on Multicast traffic on the CE puts the PXF on the PE in a loop sometimes. LDP/BGP/OSPF all go down and there is no data continuity.
CSCee11775	When Parallel Express Forwarding (PXF) forwarding fails while a debugging operation is performed you may not be able to verify the string rewrite information of the PXF engine easily.
CSCee12335	PXF buffer leak is observed when the multilink interface is flapped. Traffic must be running across the card.
CSCee14274	With Data path check feature enabled, for some reason if the data path pings fail and even though traffic is flowing through switch1 "data path feature recovery" kicks in. Data path feature recovery is to reset the card.
CSCee18100	The output drop counter of the show interface switch1 command is incorrect.
CSCee19355	The RPM-XF reloads when a service policy is applied to an interface on a card that has exceeded the packet descriptor limit.
CSCee21868	SAR buffers are getting filled up quickly.
CSCee23200	The RPM-XF throughput is reduced when cRTP/cUDP packets are being transmitted from the RPM-XF.
CSCee27588	The input packet counters for multilink interface in the show command "show pxf cpu subblock <multilink interface> are displayed incorrectly.
CSCee30230	Traffic that matches a priority class may be dropped for one single prefix. However, traffic that matches other classes may pass correctly.
CSCee37181	On RPM-XF, when there are multiple outgoing MPLS paths there could be inconsistency between hardware and software MPLS forwarding table.

Resolved Caveats—Release 12.3(2)T5

Table 4 lists the resolved caveats in Cisco IOS Release 12.3(2)T5 as of April 14, 2004.

Table 4 Resolved Caveats in Cisco IOS Release 12.3(2)T5

Caveat Number	Description
CSCed41905	DT: Automatic OIR occurred on RPM-XF card and the RPM-XF rebooted.
CSCed74712	SFP security check fails with 2-port GigE card for new SFP
CSCed48941	LSNT:PE crash with no memory for XCM temp buffer logged
CSCeb74859	DE-LSNT:BGP flap when apply/remove output policy map
CSCec14218	Trace back messages
CSCec84591	LSNT: Barium Asserted CRC error when clear int sw1
CSCec89536	LSNT: reassembler multi-bit error cause card crash
CSCed00196	RPM-XF: <show pxf tfib> doesn’t display load balanced routes
CSCed21634	Need to change exp bit on topmost label on egress interface
CSCed30548	RPM-XF - input policy map does not match against mpls exp bit
CSCed46492	Ethernet Port E2/1 on RPM-PR Card Gets Shutdown Upon Resetcd
CSCed34585	Channel ID is incorrect for certain prefixes if multi-VC is enabled
CSCed35834	LSNT: Hub router with 2 POS up links crash due to bus error
CSCed35859	Need to change the way PXF services the IP packets with option
CSCed41293	LINT:improve PXF CEF and TFIB command output
CSCed47631	sar resetinfo files don’t get written to the bootflash at times
CSCed49968	OSPF flaps between PE-LSC while congesting input hold queue
CSCed50101	Need 6s wait before turn on ATM OAM to VXSM while RPMXF GE is up
CSCed54591	Sar crashinfo does not capture event log but resets the event log
CSCed63090	RPM-XF: reload occurs when defragmenting ACL XCM memory
CSCed69526	Process sleep not allowed while interrupts are disabled.

Resolved Caveats—Release 12.3(2)T4

Table 5 lists the resolved caveats in Cisco IOS Release 12.3(2)T4 as of February 9, 2004.

Table 5 Resolved Caveats in Cisco IOS Release 12.3(2)T4

Caveat Number	Description
CSCec13765	micro code reload clears the crtp enable flag for ppoA links
CSCec09316	packet with out of range CID should be dropped
CSCec43590	RPM-XF IPHC does not decompress 16-bit paks with IP options
CSCec40662	RPM-XF reloads during <show pxf cpu rewrite tree> command
CSCec67863	RPM-XF: Memory leak when removing MDT

Table 5 Resolved Caveats in Cisco IOS Release 12.3(2)T4 (continued)

Caveat Number	Description
CSCec63848	RPM-XF: Some PXF drop counters are not cleared
CSCec31168	mVPN Tunnel receive counters not implemented
CSCec64570	Both local CEs cannot ping remote PEs, and hop count is 13
CSCeb59710	DE-LSNT:protocols flap on ELSR when withdraw LVCs
CSCec45704	LSNT:binding infor not used by tfib/cef for some PEs prefix
CSCec42547	LSNT:Incorrect MAC/Encap string in mpls forward table, traffic down
CSCeb10018	Tracebacks observed on reset card / clear ip bgp
CSCec31864	RPM-XF sending wrong fields in Interface load info VSI-S message
CSCec76217	VSICORE: Check null ptr in VprEncIfcCfgGetMore (CSCea64395)
CSCec78844	VSICORE: Check prev TCB is null before access (CSCdz38917)
CSCec39423	VSICORE: TCB Leak (CSCea20818) and unicast fixes from CSCdx87287
CSCec48318	VSICORE: TCB rel err reported incorrectly (CSCdw02481)
CSCec29812	CEF_scanner triggers high CPU util.
CSCea76134	e-iBGP load balancing does not work
CSCeb61055	Incorrect MPLS label built for VRF route
CSCea60559	lsr mib snmp agent consumes 99% cpu forever
CSCea74339	SAR-QoS: Data path VC (254/254) is not programmed properly
CSCeb80653	Generate mxt4600_info file on fatal 4700 SAR errors and reset chip
CSCec15993	In sar_mxt4400_info file, chip dump overwrites part of the data
CSCdx15989	Need debug information from sh rpm mxt4400 chip command
CSCec61293	RPMXF reloads unexpectedly deleting MPLS Switch subinterface
CSCeb47748	Display vtms info for to-RP link
CSCec60947	LSNT: AVL memory leak suspected
CSCec87123	LSNT: carrier transition counter is not working
CSCed00573	LSNT: No HWIDB_SB_C10K_TT (clear arp caused tracebacks)
CSCec53635	Channel_id is not updated sometimes after the main switch i/f resets
CSCec62846	Failure on the data forwarding path was not detected
CSCed20528	Periodic function keeps on invoking restart PVC after clear int sw1
CSCec20821	PXF reload is causing a card crash with cell-based MPLS setup
CSCeb05796	RPMXF: For a range of bandwidth, RPMXF provides lower end of range
CSCec85178	Reload due to L2 watchdog timer after microcode reload command
CSCed28880	ATM oam not tracking the gige link status on RPMXF
CSCec30428	Enhanced VTMS to Handle Possible Hardware Second Timer Update Miss
CSCed07480	IOS shows SFP MISSING for Hitachi Cable SFP
CSCec60594	Link can not be up when using 2-port POS with Y-cable redundancy
CSCed28404	PXF buffer leak occurs for tag switched packets with input policymap

Table 5 Resolved Caveats in Cisco IOS Release 12.3(2)T4 (continued)

Caveat Number	Description
CSCdy32261	traceback in config switch interface entering an incomplete command
CSCdx52061	Drop rate counter on output of sh pol int
CSCed07712	SARCMDTIMEOUT: SAR command timeout, device Reassembly SAR
CSCed33563	VSI CORE: Mem leak (ec66881) and VSI Core Code Audit fixes
CSCed31769	Multicast and output logging conflict -- (port CSCec60999)
CSCed37755	All VCs gets deconfigured in SAR after a microcode reload
CSCed15811	On data SAR fatal interrupts, SAR CMD TIMEOUTs are seen
CSCed17550	clearing pxf stat and drop counters cause mem leak
CSCec77300	RPM-XF returned to rom by bus error at rpm_send_atm_oam_cell
CSCed23216	LSNT:eiBGP multipath load balancing failed for some IP addresses
CSCec76702	Per packet load balance is not stable. Packets loss periodically
CSCed07231	rpmxf ucode error would cause protocol flags if PQ congested
CSCed07254	rpmxf ucode error would cause toaster stall error
CSCec66381	RPM-XF: SSI IPC errors during boot up
CSCeb84273	Need interrupt statistics in 2-port backcard drivers
CSCed11101	traffic cant recover after POS OIR when vrf configured on POS
CSCed35983	LSNT: Cannot CC to the RPMXF from PXM
CSCed22895	rpmc_ipc_vty.c: possible array out of boundary
CSCed22568	toaster/rpmxf-rp/rpmxf1_rp_cef.c: unmatched raise_interrupt_level()
CSCed07063	Certain sequence of ftctrace/ttctrace causes IOS crash
CSCed23982	col4_cicb_extra needs to be populated in right order
CSCec53230	Command to check consistency between ASIC forwarding & IOS TFIB
CSCed23060	Incorrect column number passed during a toaster write

Resolved Caveats—Release 12.3(2)T2

Table 6 lists the resolved caveats in Cisco IOS Release 12.3(2)T2 as of October 21, 2003.

Table 6 Resolved Caveats in Cisco IOS Release 12.3(2)T2

Caveat Number	Description
CSCea27838	SLT:SYS-3-CPUHOG trace back logged, card hang for a while.
CSCeb05118	LSNT:RPM-XF crash when delete sw1.1 mpls interface
CSCea60343	LSNT: connection goes into mismatch
CSCdw45040	RPM-XF comes up with partial configuration
CSCdw76205	Error messages when deleting the sw conn under PVC.
CSCdw86377	Attempting to conf a partition with more lcns than MAX causes TrBack

Table 6 Resolved Caveats in Cisco IOS Release 12.3(2)T2 (continued)

Caveat Number	Description
CSCdw86381	cnfpnportcac causes traceback if bw used is greater than min bw req
CSCdx06018	TMC: Multiple VBR flows hash to same toaster Q. Cause taildrops.
CSCdx92871	iBGP load balancing does not work when two ces are in different vpns
CSCdy05346	Missing param-groups in Sw Get Cnfg Rsp VSI slave message
CSCdy17457	sh int shows wrong packet number after shut/no shut the interface
CSCdy26882	Interface counters show incorrect values after backcard OIR
CSCdy42274	PXF doesn't recover after a reload at high traffic rates
CSCdy73751	Certain HW error interrupts may cause the Tx GigE traffic to stop
CSCdz23621	Z-RED: Standby RPM-XF vsi master endpoint id is not cleared on PXM
CSCdz86609	Packet drop was observed at switch interface1 when traffic flowing through
CSCea15938	GTS shapes too aggressively for POS/GigE interfaces

Compatibility Notes

RPM-XF Boot File and Firmware File Names and Sizes

The following table displays the RPM-XF boot and firmware file names and sizes for this release.

Table 7 RPM Boot and Firmware File Names and Sizes

	File Name	File Size (in bytes)
Boot File	rpmxf-boot-mz.123-7.T3	3448088
Firmware File	rpmxf-p12-mz.123-7.T3	9415796

RPM-XF Compatibility Matrix

Table 8 RPM -XF Compatible Software Versions

MGX SW version	3.0.10	4.0.10	4.0.12	4.0.15	5.0.00	5.0.00	5.0.10
IOS Version	12.2.15T	12.2(15)T5	12.3(2)T2	12.3(2)T4	12.3(2)T5	12.3(2)T6	12.3(7)T3
CWM	11.0.10	12.0.00.1	12.0.00.2	12.0.00.2	15.0.00	15.0.00	15.0.00 P2

MGX RPM-XF Hardware

Table 9 shows the front card and back card compatibility for the RPM-XF hardware supported in this release. The table lists the card model/ name, part numbers, the minimum version and the minimum revisions of each card supported. Note that there may be more than one 800 level part numbers for the same front cards. The minimum version is identified by the last 2 digits of the 800 level numbers.

Table 9 Hardware Compatibility Matrix

Front Cards	Part Number/ Min. Version	Rev.	Back Cards	Part Number/ Min. Version	Rev.
MGX-RPM-XF-512	800-09307-03	A0	MGX-XF-UI	800-09492-01	A0
			MGX-XF-UI/B	800-24045-01	A0
			MGX-1GE	800-18420-03	A0
			MGX-2GE	800-21300-04	A0
			MGX-1OC12POS-IR	800-08359-05	A0
			MGX-2OC12POS-IR	800-20831-04	A0

Table 10 SFP Compatibility Matrix for MGX Gigabit Ethernet and POS Back Cards

SFPs	Part Number/ Min. Version	Rev.
GLC-SX-MM (was MGX-GE-SX)	30-1301-01	A0
GLC-LH-SM (was MGX-GE-LHLX)	30-1299-01	A0
GLC-ZX-SM (was MGX-GE-ZX))	10-1439-01	A0

Cisco IOS Release Compatibility Information

All IOS firmware can be downloaded from CCO from the following location:

http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml

Using XModem to Download Flash to RPM-XF Cards

Use the xmodem feature to download the flash to an RPM-XF card. During this process, the card should be connected to a target machine through HyperTerminal with settings of 9600, n, 8, and 1.

Step 1 Put the node in monitor mode by entering the **priv** command to gain access to the privileged commands as follows:

```
rommon 1> priv
You now have access to the full set of monitor commands. Warning:
some commands will allow you to destroy your configuration and/or
system images and could render the machine unbootable.
```

Step 2 The xmodem command becomes available and the general syntax of this command and availability of this can be checked by giving xmodem command without any parameters on the CLI, as follows:

```
rommon 2 > xmodem
usage: xmodem [-cy]
-c  CRC-16
-y  ymodem-batch protocol
rommon 3 >
```

The command line options for xmodem are as follows:

Option	Definition
–c	xmodem performs the download using CRC-16 error checking to validate packets. Default is 8-bit CRC.
–y	xmodem uses Ymodem-batch protocol for downloading, which uses CRC-16 error checking.

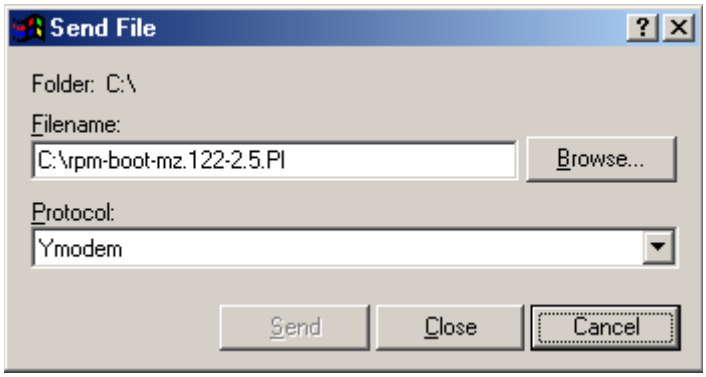
Note If you do not find the xmodem commands, then the xmodem feature is not available on this rommom version. In that case, you must return the card to Cisco.

Note The rommon “xmodem/ymodem” transfer only works on the console port. You can only download files to the router. You cannot use “xmodem/ymodem” to get files from the router.

For example:

```
rommon 4> xmodem -cy
Do not start sending the image yet...
Invoke this application for disaster recovery. Do you wish to
continue? y/n [n]: y
```

Step 3 Use the Transfer-->Send File option in HyperTerminal to start the image transfer.



In the Filename box, browse and choose the image file to be downloaded. Also since we used the “y” option while invoking the xmodem, set the transfer protocol to ymodem or use Xmodem protocol by not specifying the –y option on the command line.

The transfer screen comes up and transfer starts. (The transfer may not start immediately; wait for some time and it should start.)

The system will reset itself from here and will boot with new software image.

Historical Information for 12.2.x IOS Baseline

Resolved Caveats—Release 12.2(15)T5

Table 11 lists the resolved caveats in Cisco IOS Release 12.2(15)T5.

Table 11 Resolved Caveats in Cisco IOS Release 12.2(15)T5

Caveat Number	Description
CSCeb06375	**Symptom:** An access list may fail to work as configured. **Conditions:** This symptom may be observed when virtual circuits (VCs) are torn down and recreated. The symptom occurs after the switch subinterface is shut down and then brought up. **Workaround:** Remove the access list and add it again.

Table 11 Resolved Caveats in Cisco IOS Release 12.2(15)T5 (continued)

Caveat Number	Description
CSCea49948	**Symptom:** Multiple crashinfo files may be saved on a Cisco Route Processor Module XF (RPM-XF) because of a reused IPC buffer (a second IPC send). If multiple crashinfo files are generated, the available storage space in the bootflash might get all consumed. If the card is part of a redundant pair, the card may fail during an attempt to switch back to the primary card from the secondary card in the redundant pair. **Conditions:** The symptom is observed when a switchover occurs from an RPM-XF to the redundant RPM-XF. If there is not enough bootflash free storage space available to load the configuration file, RPM-XF card might not go to Active state. After multiple switchover attempts, the Processor Switch Module (PXM) marks the first RPM-XF as failed. **Workaround:** Delete some crashinfo files to clear space on the bootflash before attempting to switch back to the active RPM-XF card.
CSCea93735	**Symptom:** Control traffic may not be dequeued from a Parallel Express Forwarding (PXF) processor towards a Route Processor (RP). **Conditions:** This symptom is observed on a Cisco MGX 8800 series Route Processor Module XF (RPM-XF) in a Multiprotocol Label Switching (MPLS) environment. In a cell-based MPLS network, the symptom occurs when an MP LS packet with a Time To Live (TTL) setting below 2 reaches a provider edge (PE) router. In a frame-based MPLS network, the symptom occurs when an MPLS packet with explicit null labels and with a TTL setting below 2 reaches a provider (P) or PE router. **Workaround:** Configure the "no mpls ip propagate-ttl" global configuration command on all the routers in the MPLS network to prevent MPLS packets with a TTL setting below 2 from being generated.

Resolved Caveats in Release 12.2.15T

Table 12 lists the resolved caveats in Cisco IOS Release 12.2.15T.

Table 12 Resolved Caveats in Cisco IOS Release 12.2.15T

Caveat Number	Description
CSCea49948	**Symptom:** Multiple Crashinfo due to IPC Messages. Multiple crash info files are generated, filling the bootflash of RPM-XF card. **Conditions:** It may happen due to polling that involves IPC communication between Processor Switch Module 45 (PXM45) controller and RPM-XF card. RPM-XF switchover may lead to this issue. **Workaround:** None
CSCdz82543	**Symptom:** Cannot cc to RPM-XF due to Messages on the Console. You may not be able to log into a Cisco Route Processor Module XF (RPM-XF), although when you display the status of the module from a Processor Switch Module 45 (PXM45) controller, no irregularities are shown. If you manage to establish a console connection into the RPM-XF, continuous traceback messages may be displayed on screen. **Conditions:** These symptoms are observed when RPM-XFs are installed in an MGX45 shelf, Cisco WAN Manager is configured to poll the RPM-XFs for statistics and scripts run on the node that log into every module sequentially. **Workaround:** None
CSCdx08155	**Symptom:** On LSC, querying of lvc statistics for an xtagatm interface would not abort command upon user entering a ctrl-c. If user use "show xtagatm cross-connect traffic" to query on lvc statistics, normally, user can quit the command in the middle by giving the ctrl-c sequence. However, the CLI would not return the prompt until the VSI Master logic complete requesting statistics for all lvcs. **Conditions:** If the number of lvcs on LSC is small, user may not be able to notice the impact. However, if the number of lvcs reach a few thousands (i.e. 4000 lvcs), user may experience no response from the cli session up to 2-3 minutes. But the rest of the system will still function normally. **Workaround:** If user needs to query on lvc statistics, try to let the command run to completion. Avoid aborting the command in the middle of execution with ctrl-c.

Table 12 Resolved Caveats in Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy26703	**Symptom:** A ping from a customer edge (CE) to a provider edge (PE) may fail, and Parallel Express Forwarding (PXF) may stall. **Conditions:** These symptoms are observed on an MGX Route Processor Module (RPM) that is installed in a Cisco MGX 8000 series switch that is functioning as a PE router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network and that has VPN routing/forwarding (VRF) enabled on the virtual template. The PE router is connected to the CE router via a PPP over ATM (PPPoATM) link. PXF may stall even though the PPPoATM session is established. **Workaround:** None
CSCdy27120	**Symptom:** Traffic doesn't flow thru a VLAN on GigE interface **Conditions:** If a shutdown is executed on an interface before defining the encapsulation type, traffic might not flow thru a VLAN on a GigE interface. **Workaround:** On the VLAN interface, disable and re-enable the encapsulation.
CSCdy65600	**Symptom:** The output and input flow control parameters of a Gigabit Ethernet interface are displayed as ? "aused".? **Conditions:** This symptom is observed on the Gigabit Ethernet interface a Cisco router that has auto-negotiation enabled. **Workaround:** Disable auto-negotiation on the Gigabit Ethernet interface.
CSCdz70762	**Symptom:** Multi-vc traffic coming on a particular precedence goes out to a queue with wrong precedence. **Conditions:** The mac rewrite string is found to be incorrectly configured. **Workaround:** None

Table 12 Resolved Caveats in Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdz82543	**Symptom:** You may not be able to log into a Cisco Route Processor Module XF (RPM-XF), although when you display the status of the module from a Processor Switch Module 45 (PXM45) controller, no irregularities are shown. If you manage to establish a console connection into the RPM-XF, continuous traceback messages may be displayed on screen. **Conditions:** These symptoms are observed when RPM-XFs are installed in an MGX45 shelf and Cisco WAN Manager is configured to poll the RPM-XFs for statistics, causing scripts to run on the node and log into every module sequentially. **Workaround:** None
CSCea05477	**Symptom:** After policy map is created, RPM-XF reset. **Conditions:** Created a policy map with police option with CIR rate configured to 125000000 and bc configured to 20000 for confirm action and exceed action was drop. Soon after creating policy map it gave `Conform burst size increased to 62500` and card resetted. **Workaround:** None
CSCin32860	**Symptom:** Access list info of snmp-server community lost after RPM-XF reset **Conditions:** After RPM-XF is reset , the access list info of the snmp-server community is lost. **Workaround:** After RPM-XF is reset, re-configure the snmp-server community string as required on RPM-XF.

Resolved Caveats Prior to Release 12.2.15T

Table 13 lists the resolved caveats prior to Cisco IOS Release 12.2.15T.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T

Caveat Number	Description
CSCdw20568	Symptom: Cisco Class-Based QoS mib - CISCO-CLASS-BASED-QOS MIB - is not supported on RPM-PR and RPM-XF. Conditions: SNMP walk on CISCO-CLASS-BASED-QOS mib on RPM-PR and RPM-XF cards return no values for mib objects. Workaround: None.
CSCdw55382	Symptom: The output of the command **sh swi conn vcc/vpc** doesn't show the value of the maximum cost field correctly. Conditions: Maximum cost was configured explicitly on the master endpoint of the connection to a value of 4294967295 i.e. 0xFFFFFFFF. Workaround: Use **dspcon** command on the PXM to look at the configured value.
CSCdw57105	Symptom: Show sub-interface counter shows incorrect value. Conditions: When there is some drop on the sub-interface, value becomes negative, causing the numbers to be incorrect. Workaround: Issue **clear counter** command.
CSCdw68738	Symptom: Cobalt From RP Own Errors counter increments in **show hard pxf dma count** output. This does not affect data/traffic. Conditions: Spontaneous increments of these counters have been noticed always with no specific side effect. Workaround: None

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description

CSCdw69661	Symptom:
	Invalid Epid Error message seen.
	`00:00:10: %P2IPC-4-COMEPDELETED: ssi_ipc_epid_idx_validate()`
	`Non-existing CommEp 60010F8 has invalid tag 4096;`
	`Expected tag is 0`
	`-Process= "P2IPC Receive Process", ipl= 0, pid= 17`
	Conditions:
	After RPM-XF switchover, standby card prints invalid Epid Error messages as VSI Slave Epid on Standby is not in use.
	Work around:
	None
	Further problem description:
	The error messages are harmless traceback as it happens on the Standby card.

CSCdw88019	Symptom: Loopbacks provided on GigE backcard should be renamed to 'internal' and 'external' from 'mac' and 'driver', respectively Conditions: Previously, RPM-XF software used "mac" and "driver" as loopback command parameters to mean internal and external loopbacks respectively. These parameters have been replaced by "internal" and "external" as loopback command parameters. Workaround: Use **show controllers gigabitEthernet 1/0** command and user documentation to correlate the loopback type with the loopback configuration.
CSCdw88767	Symptom: Humvee counters show improper value and counters cannot be cleared. Conditions: While traffic is passing through, counters wrap around and become negative. Workaround: None.
CSCdw95563	Symptom: After increasing the PCR value of PVP, traffic is getting dropped at new rate. Conditions: When PCR value is changed, it does not take affect so VP is still shaped at old rate. Workaround: Delete the VP and readd it.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdx00982	Symptom: SNMP **get** returns a different value for pcr/scr from what was configured. Conditions: The connection was added through CWM/SNMP with a value such that on conversion from cps to kbps and then back to cps does not give back the original cps value. Workaround: While adding connections through CWM/SNMP, do not use such values (in cps) for scr/pcr for which conversion from cps to kbps and then back to cps does not give back the original value.
CSCdx12730	Symptom: All the PVCs on the switch1 interface go to INACTIVE state. Conditions: Any destructive command can cause this condition. Some of them are: 1. **clear interface switch1** command was issued. 2. Modification of the atm pvp tunnel. 3. Changing MTU value of Switch1 interface or sub-interface. Workaround: Issue **clear interface switch1** command.
CSCdx16897	Symptom: Performance issue observed in cleaning up and creating LVCS. Conditions: With RPM-XF as headend eLSR, it takes about 1 minute to cleanup and recreate 500 LVCS. Workaround: None

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdx44836	Symptom: Modifying an existing PVP may cause the following VSI error to be displayed on console or logged: `04:57:14: %VSI_VRM-4-GENERR_NUM: VSIRmGetXConnectInfo, line 6658: Vsis RM error <Failed to search Vco database for lcn =>>, info=1` Conditions: This error only happens if the existing PVP has a configured switch-conn-vpc but is not routed yet (only slave end is added). This error is informational only to indicate that there is no remote cross-connect information to be returned because the vpc is not routed yet. There is no service impact. Workaround: Complete the VPC connection by adding the remote end.
CSCdx46583	Symptom: Need to verify IOS images on PXM Hard Drive and in RPM-XF Flash. Conditions: In order to do the health check of the IOS images on PXM Hard disk & Bootflash, a new CLI command is being introduced: **debug rpm check_image now x:**<*image-name*>. Workaround: None.
CSCdx49122	Symptom: **dspcd** <*slot#*> for RPM-XF slot doesn't show the full CLEI code / Serial number. One character at the end is missing. Conditions: When **dspcd** command is executed on PXM. Workaround: **cc** to RPM-XF card and do **sh rpm cdmgmt scmExtPollInfo** to find the correct CLEI code and Serial number.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdx52025	Symptom: Could not correlate output packets dropped on sub-interface with switch1 interface packet drop counters. Conditions: Sub interface counters don't have any drop counters, so if any packet is dropped on a particular sub-interface, it is shown on switch1 interface but not on that sub-interface. Workaround: Use **sh atm pvc** <*vpi/vci*> to see all the drops.
CSCdx55586	Symptom: Setting ccCopyEntryRowStatus to ACTIVE returns "general error" status even if the row is correctly configured. Conditions: Attempting to use the CISCO-CONFIG-COPY-MIB to copy a configuration file. Workaround: None.

CSCdx58504	Symptom:
	RPM-XF **show switch conn vcc|vpc** displays NSAP in following format:
	`47.0091.8100.0000.0001.6443.6c58.0000.0109.1802.00`
	which is not consistent with PXM **dspcons** display.
	Conditions:
	RPM-XF "**show switch conn vcc|vpc**" displays NSAP in following format:
	`47.0091.8100.0000.0001.6443.6c58.0000.0109.1802.00`
	which is not consistent with PXM "**dspcons**" command output:
	`47.009181000000000164436c58.000001091802.00`
	Workaround:
	None.

CSCdx62385	Symptom: flapping of BGP causes RPM-XF reload. Conditions: The reload happened after the routes exceeded 102K vrf route limit and **clear ip bgp *** is executed. Workaround: Do not exceed the given limit of Maximum number of vrf routes which is 102k.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdx64337	Symptom: After changing the console baud rate the console may behave unpredictably. Conditions: The console responsiveness is unpredictable. You may need to hit enter many times to get a prompt back. Workaround: Avoid changing the baud rate of the console port. To recover from the erratic console behavior, you will need to perform a system reload.
CSCdx64361	Symptom: ROMMON console can lock up after pasting a large buffer. Conditions: The ROMMON console driver can run out of descriptors with a sufficiently large paste buffer (~1k). After this happens, the console appears hung. Workaround: Paste data to the ROMMON console in increments less than 1k. Once the ROMMON console driver runs out of descriptors, the only way to recover is to perform a system reset or power cycle.
CSCdx69702	Symptom: The output counters displayed under **show policy-map int** <*sw1.x*> are not incremented. Conditions: When an output service policy is applied to a subinterface and the policy map includes class maps with no actions. Workaround: Either do not configure class maps with no actions or rearrange the class maps within a policy map so the class maps with no actions are last.
CSCdx71190	Symptom: A software-forced reload may occur on a router, and the Open Shortest Path First (OSPF) process may fail. Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(10.7)T1 and that is configured for Border Gateway Protocol (BGP) tag switching with OSPF in an autonomous system. The router may reload when the main link bandwidth is changed to switch to the shortest path. This behavior may cause the router OSPF process to fail. Workaround: There is no workaround.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdx76951	Symptom: There was humvee error on RPM-XF card. Conditions: When ever switchcc is done or card comesup, humvee generates some errors. These errors are harmless, unless they are incrementing coutinously. Workaround: None.
CSCdx80500	Symptom: A CLI command is needed to show the history of the messages that RPM-XF received from the Shelf Manager on PXM. Also, a second command is needed to clear this log. Conditions: NONE Workaround: None
CSCdx87265	Symptom: Deletion trap is not sent out for notOnRpm connections. Conditions: RPM-XF reset or switch over before provisioned connections get saved into configuration. Workaround: None.
CSCdx91454	Symptom: The status LEDs for the management backcard are not illuminated correctly. Conditions: When the boot image is used, the status LED on the back of the management back card is not illuminated as it should be. With the system image status LED on the back of the management back card is illuminated but the LM1OK LED on the front card is off instead of green. Workarounds: Use the 's**how interface FastEthernet2/0**' and '**show interface FastEthernet2/1**' commands to view the status of the management backcard.
CSCdx93773	Symptom: Packet drop on egress sub-interface below configured rate. Conditions: Sending traffic at SCR rate on a vbr pvc with high SCR value configured. Workaround: None

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy02182	Symptom: When the GigabitEthernet device driver detects an error with the link to the front card, it does not automatically try to correct the situation properly. Conditions: When the GigabitEthernet device driver detects an error with the link to the front card you may see messages similar to: `BARIUM ERROR EVENT: send reason 7 slot 1` The device driver should then try to reset the link to the front card and continue but does not. Workaround: When you receive an error message similar to the one described in conditions, you should shutdown and restart the interface to clear the condition.
CSCdy03275	Symptom: Traffic is not passing in frame-based MPLS network when RPM-XF is configured as P router Conditions: RPM-XF configured as P router. Workaround: None
CSCdy05871	Symptom: Tail drops on PXF queue while sending traffic at OC12 rate. Conditions: Configure interface speed as more than 500Mbps (X) and send more than X/2 single flow traffic Workaround: Use multiple flows (different source-destination)
CSCdy09544	Symptom: LLQ (Low Latency Queue) starves low priority traffic. Conditions: Traffic exceed configured bandwidth for the LLQ, but still below the configured SCR (Sustain Cell Rate). There are drops on other low priority classes even though they are in their configured limit. Workaround: None

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy11581	Symptom: Received traps for "Fast Ethernet Interface Down(60662)" and "Fast Ethernet Interface up(60661)" have incorrect *ifName* contents. Conditions: Generate "Fast Ethernet Interface up(60661)" by doing admin up on interface and notice the contents of "*ifName*" in the trap PDU on CWM or any other SNMP trap client. Do the same for "Fast Ethernet Interface Down(60662)" by doing admin down on the interface. The contents for "*ifName*" is "**FastEthernet/12/0**". The correct value should be **FastEthernet/**<*log-slot*>/<*bay*>/<*port*>. Workaround: None.
CSCdy15295	Symptom: cbQosQueueingStats and cbQosREDClassStats MIB entries are not populated. Conditions: SNMP mib walk on RPM-XF for cbQosQueueingStats and cbQosREDClassStats mib objects return no entries. Workaround: None.
CSCdy23757	Symptom: Data stops flowing from VLAN after removal and insertion of GigabitEthernet backcard is done. Conditions: After removal and insertion of GigabitEthernet backcard, data traffic from the configured VLAN stops. Workaround: Perform **`no encaps dot1q**' on the VLAN interface and then re-add all the configuration defined on that VLAN.
CSCdy26495	Symptom: class-map output queue packet counter doesn't show the correct number of packets. Conditions: With policy-map attached, send the traffic with the rate not to see drops Workaround: Use the class-map total number of packet counters.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy26755	Symptom: Execution of PXM command "**dspcd**" for the RPM-XF card does not show 800 Level Rev number for the frontcard and the backcard Conditions: Execution of PXM command "**dspcd**" on a particular slot, even when backcard and front card is present, the 800 level Rev information is blank. Workaround: `**cc**' to RPM and use the command `**sh rpm eeprom**'
CSCdy27852	Symptom: Excessive delay for LLQ packets. Conditions: Send LLQ packets during congestion of the non LLQ queues. The issue only happens for vbr-nrt connections with rate <= 128 kbps, if excessive traffic is pumped on queues other than LLQ and default queue. The issue would happen for all rates if excessive traffic is pumped on the default queue. Workaround: none
CSCdy28132	Symptom: Traffic forwarding stops. You may see the traffic forwarded to the wrong VC. Conditions: Shut followed by no shut on the MPLS interface with multi-vc could lead to this issue. This is an intermittent issue. This could also happen if the LVCs go down and come back up for any other reason. The issue is seen only with VRF prefixes. Workaround: shut/no shut the interface. If problem persists, switch to a redundant card if one is available.
CSCdy30260	Symptom: Protocol flap is observed and data labeled transfer stops temporarily on RPM-XF when RPM-XF card in adjacent slot is removed. Traffic resumes after around 100 seconds. Conditions The issue happens when RPM-XF card in the adjacent slot is pulled out, the RPM-XF cards being in one of the following pair of slots: (1,2), (3,4), (5,6), (9,10), (11,12), (13,14), (15,16). (MGX 8850) (1,2), (3,4), (5,6), (11,12), (13,14), (15,16). (MGX 8950) This happens with or without 1:N redundancy. Workaround Do not use RPM-XF cards in adjacent slots with combination as above.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy31406	Symptom: RPM-XF frame-based P router's PXF reloaded after "shut" PE subinterface. Conditions: RPM-XF configured as P router. Upon "shut" on PE's subinterface, PXF module on P router got reloaded. Workaround: None.
CSCdy37576	Symptom Cannot add a dax connection between the RPM-XF (10) and the AXSM (1) Condition From the PXM perspective, the available CPS on the axsm is different than that of the rpm-xf. however when i am picking the lower value to add the pvc the pvc is still failing to add. the rpm-xf is showing reason as no resources. Work-around Unknown
CSCdy38362	Symptom: Line Alarm seen on Gigabit ethernet interface on MGX-1GE even when administratively down. Conditions: If interface was in alarm prior to being shutdown, it continues to persist even after the shutdown. Workaround: Doing a 1:N redundancy switch over (if redundancy is configured) to the standby RPM-XF clears this alarm on the card and at the node level. This is to be done after the Gigabit Ethernet interface is shutdown, and a "**write mem**" has been done on the active. The alarm can be cleared by regular means such as ensuring proper cabling, SFP type match with other end, and administratively enabling other end prior to shutting down this end. If the other end is also not running the same software release that includes this bug then the alarm will move to the other end on trying such workaround. If redundancy is not configured, resetting the front card (disruptive) would be needed to clear the alarm.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy39423	Symptom: Traffic stops going out on GigE interface when enabling autonegotiation parameter. Conditions: With traffic flowing, if *autonegotiation* parameter is enabled on GigE interface, traffic may stop. Workaround: shut/no shut on the GigE interface
CSCdy39806	Symptom: "No switch partition configured" trace back error logged. Conditions: Setup eLSR with vp tunnel mode on RPM-XF Workaround: None
CSCdy39861	Symptom: Spurious memory trace back error logged when disable VRF forwarding under switch sub-interface Conditions: Disable VRF forwarding under switch sub-interface on RPM-XF LER Workaround: None
CSCdy40930	Symptom: LLQ packets dropped on SAR because of lack of buffers Conditions: Congest the pvc with the LLQ traffic Workaround: none Further problem description: The scheduler calculates the time it took to send a burst of traffic on a VC. This calculation results in an integer value which is a rounded down of the actual value. This rounding causes error in the scheduling time, which causes shaping inaccuracy. The fix is to try to keep the rounding error to a minimal.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy41773	Symptom: In case of GIGE backcard initialization failure, further configuration on it may cause the RPM-XF card to reboot. Conditions: If the GIGE backcard initialization fails, loading start-up config or manual configuration that changes the uninitialized GIGE backcard configuration, might cause RPM-XF to get reset. Workaround: None
CSCdy45515	Symptom: Connection endpoint on RPM-XF Does Not Generate RDI Upon Receiving AIS Conditions: RPM-XF endpoint of a xpvc does not generate RDI upon receiving AIS. The RPM-XF atm pvc erroneously reports that RDI is generated. However, a display of the connection count at the corresponding AXSM on the node indicates that the RDI is, in fact, NOT generated. Workaround: unknown
CSCdy51893	Symptom: Class queues do not get programmed correctly.CBWFQ may not work correctly. Conditions: Modify the policy map values associated to a particular subif. Workaround: shut/no shut on sub-interface
CSCdy53728	Symptom: LLQ when defined with class queues does not achieve full SCR and also improper traffic distribution between the queues. Conditions: With less traffic on class queues and more traffic on LLQ and with rates such that SCR is congested, its observed that the bandwidth is not being shared accurately among the queues as per the ratios assigned to them. LLQ sometimes get less traffic or more traffic and its not deterministic. Workaround: Enable MaxUtilization and OverSubscription on LLQ and Class Queues.

Table 13 Resolved Caveats Prior to Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCdy55202	Symptom: **sh pol int** shows zero bandwidth for all the classes. Conditions: When ever class default is configured with some bandwidth and policy is removed and reattached, all other class bandwidth becomes zero. This happens for mpls interfaces. Workaround: None.
CSCdy56345	Symptom: After removal and insertion of POS backcard, `Assertion Failure' tracebacks were observed. Conditions: When a policy map is configured on POS i/f and removal and insertion of the POS backcard is done, "Assertion Failure" tracebacks will be observed on the console window. Workaround: Remove the policy map and reapply it on the POS i/f. Further Problem Description: The issue is applicable to GigE backcard also.
CSCdy71426	Symptom: All the traffic on PXF stops. Conditions: If a service policy was attached to an interface, with no bandwidth leftover for default class. Any traffic pumped on this interface default class would cause PXF to freeze and hence stopping traffic. Workaround: Reconfigure the policymap to have some bandwidth for class-default and then reload the PXF microcode using 'micro reload pxf'.
CSCdy75485	Symptom: All Layer 2 management packets are dropped, which causes all interfaces that depend upon keepalives to transition to the down state. Conditions: This symptom is observed on a Cisco 10000 series router in a configuration with a large numbers of interfaces. Workaround: Unknown

Related Documentation

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

Note that for this release, in addition to the RPM-XF user documentation (*Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*) use the MGX Release 5 and Cisco IOS documents as well as this release note.

Product documentation for the PXM45-based MGX 8850 is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/rel5/index.htm

Product documentation for the PXM45-based MGX 8950 is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8950/rel5/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from 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 may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

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

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

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 Networking Products MarketPlace:

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

- 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 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

This document is to be used in conjunction with the Cisco WAN Switching publications.:
Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4

Copyright © 2004 Cisco Systems, Inc.
All rights reserved.