Release Notes for Cisco MGX Route Processor Module (RPM-XF) Cisco IOS Release 12.4(6)T1 for PXM45-based Switches, Release 5.3.00

Part Number OL-8893-01 Revision A1, May 26, 2006

Contents

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

Overview

These release notes contain the following sections:

- "About this Release" section on page 4
- "New Features" section on page 4
- "RPM-XF Redundancy Support" section on page 22
- "Features Not Supported in Cisco IOS Release 12.3(11)T7" section on page 23
- "SNMP MIB" section on page 23

About this Release

These release notes describe the system requirements, new features, and limitations of the Cisco MGX Route Processor Module (RPM-XF) Cisco IOS Release 12.4(6)T1 for PXM45-based Switches, Release 5.3.00. These notes also contain Cisco support information.

For more information on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 5.2*.

New Features

This section lists new features (introduced by release) for the Cisco MGX Route Processor Module (RPM-XF) Cisco IOS Release 12.4(6)T1 for PXM45-based Switches, Release 5.3.00 or earlier.

Features Introduced in Cisco IOS Release 12.4(6)T1

Features added to the RPM-XF in Cisco IOS Release 12.4(6)T1 include:

- Secure Shell (SSH) Console
- SAR Enhancements
- Control Plane Policing
- Bidirectional Forwarding Detection
- Offline Diagnostics

Secure Shell (SSH) Console

Secure Shell (SSH) is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The application is similar to the Berkeley rexec and rsh tools. The protocol secures the sessions using standard cryptographic mechanisms. Two versions of SSH are available: SSH Version 1 and SSH Version 2. Cisco IOS Release 12.4(6)T1 implements SSH server and client for both versions. You must have the RPM-XF crypto image installed to use the SSH feature.

The SSH feature on the RPM-XF is useful if you want to manage the card through its management or high-speed back card. More often however, you manage the RPM-XF, and all other cards in the MGX chassis, from the PXM45 controller. The PXM45 controller also implements SSH and provides the same level of security.

If you plan to use SSH on the RPM-XF, consider disabling telnet access to improve security. Telnet transfers all user ID, password, and session management information between the client and the RPM-XF using clear text. Clear, or unencrypted text can be read by network analysis and snooping tools.

Note The RPM-XF must have the crypto image installed to use the SSH feature.

For software image information, refer to Compatibility Notes, page 64

SSH Configuration Guidelines

To use SSH the first time, you must activate the SSH server. You can then enable or disable SSH, or other management protocols, on the asynchronous (vty) ports. You enable the SSH server and configure SSH ports on the RPM-XF as you would other Cisco routers running Cisco IOS Release 12.4(6)T1.

The RPM-XF stores crypto keys in a secure way on the PXM hard disk. This is necessary to support 1:N redundancy for RPM-XF cards. The PXM card stores the crypto key for each RPM-XF in the following directory and file:

E:/RPM/private_config_slotnn

where nn is the two digit logical slot number

Note Do not remove or modify the crypto key file; doing so disables SSH on the RPM-XF.

For more information about configuring SSH, refer to:

- Cisco IOS Security Configuration Guide, Release 12.4

Management Port Configuration Guidelines

All management sessions to the RPM-XF, including those initiated with the **cc** command at the PXM card, utilize the asynchronous (vty) ports. In Release 5.3.00 the RPM-XF supports up to 250 vty ports (CSCsd05487).

Note Earlier releases supported up to 1000 vty ports.

You allocate vty ports among the management protocols you plan to use:

- ssh
- rlogin
- telnet
- rpm ipc
- all
- none

You assign protocols to vty ports using the **transport** command (See SSH Commands). Always configure a few vty lines for **rpm ipc**, so you can manage the RPM-XF from the PXM card. Then, configure other vty lines for the protocols you plan to permit on backcard interfaces.

Note You must enable at least one line for **rpm ipc** to manage the RPM-XF from the PXM.

The following example configures three ports for rpm ipc and two for ssh:

```
line vty 0 2
 password cisco
 login
 transport input rpm ipc
 transport output rpm ipc
line vty 3 4
 password cisco
 login local
 transport input ssh
 transport output ssh
```

In this example, the **login local** command specifies that ssh should use a local database of users. In a production environment, you would usually use an authentication server instead.

SSH Commands

The SSH feature in Cisco IOS Release 12.4(6)T1 adds the following global configuration commands to the RPM-XF:

- **crypto key generate rsa** (only RSA keys are supported)
- **ip ssh**

The SSH feature also adds the following user exec commands:

- **show crypto**
- **show ip ssh**
- **show ssh**

The SSH feature extends the following line configuration command:

- **transport** {**input** | **output**} {**rpm ipc** | **all** | **none** | **rlogin** | **ssh** | **telnet**}

The RPM-XF extends the standard **transport** command to include the **rpm ipc** option, which supports internal management sessions with the PXM card.

For command reference information, refer to the following:.

- Cisco IOS Master Commands List, Release 12.4

SAR Enhancements

This section describes the segmentation and reassembly (SAR) performance enhancements for the RPM-XF.

SAR Buffer Pool Allocation

Release 5.3.00 introduces the **atm sar-buffers tx** configuration command under **interface Switch1**. Releases earlier than 5.3.00 statically allocate SAR buffers to the UBR, VBR and LVC classes in the ratio of 1:2:1. Static allocation leads to under-utilization of buffers in some cases. When the traffic on an RPM-XF is predominantly VBR, this under-utilization can lead to reduced tolerance for bursty traffic. You use the **atm sar-buffers tx** command to reallocate the total SAR buffers between UBR, VBR and the LVC classes based on expected usage for these traffic classes (See atm sar-buffers tx, page 38**).**

To display the buffer pool allocation and usage counters, enter the **show controllers Switch1** command. This command displays the in-use /allocated buffers for each of the three classes.

```
RPM-XF_SF#show controllers switch 1 sar
Interface Switch1 is up
...
Data Path SAR buffer usage statistics:
Data Res SAR Class 1 current buffer usage: 0x00000002 / 0x00054000
Data Res SAR Total current buffer usage : 0x00000002 / 0x00054000
Data Res SAR Total buffer usage ratio : 000%
Data Seg SAR Class 1 current buffer usage: 0x00000003 / 0x00015000
Data Seg SAR Class 2 current buffer usage: 0x00000001 / 0x0002A000
Data Seg SAR Class 3 current buffer usage: 0x00000000 / 0x00015000
Data Seg SAR Total current buffer usage : 0x00000004 / 0x00054000
Data Seg SAR Total buffer usage ratio : 000%
...
RPM-XF_SF#
```

SAR Cumulative Queue Size Counters

The SAR cumulative queue size counters display the sum of all queue size configurations of the VCs belonging to a traffic class. These counters, in conjunction with the buffer pool usage counters, provide information about over-subscription, if any.

To display the cumulative queue size configuration for each class and detect potential oversubscription of buffer classes, enter the **show controllers switch 1** command. (CSCei21134)

```
RPM-XF_SF#show controllers switch 1 sar
Interface Switch1 is up
...
Data Seg SAR cumulative queue size per buffer class:
Data Seg SAR Class 1 cumulative queue size  : 0x000003C0
Data Seg SAR Class 2 cumulative queue size  : 0x00007C80
Data Seg SAR Class 3 cumulative queue size  : 0x00000000

Data Seg SAR Total cumulative queue size    : 0x00008040

...
RPM-XF_SF#
```

SAR CoS Queue and Weight Allocation

This release improves the CoS weight calculation to overcome the deficit counter wrap issue. The weight of a cosq controls the average number of cells a cosq services at each turn. The deficit counter keeps track of the actual number of cells serviced at each turn. If a wrap-around of the deficit counter occurs, it can cause inconsistencies in bandwidth distribution between classes of a service policy. Release 5.3.00 resolves this problem.

SAR 1.4 Upgrade

This release integrates the new GA version of SAR ucode from Mindspeed, which has backward support for version 1.3. This new version has critical bug fixes.

Control Plane Policing

Control Plane Policing (CoPP) increases router security by protecting the route processor from unnecessary and potentially malicious traffic. The route processor handles important and time critical packets, such as layer 2 and layer 3 keep alive messages, routing protocol updates, control protocol, network management, and other process level tasks related to control plane operation. Without CoPP, the control and management planes can be vulnerable to high rates of undesirable traffic that can interfere with routing stability, reachability, and packet delivery.

Note The RPM-XF does not support control plane protection options host, cef-exception, or transit.

CoPP Configuration Guidelines

You enable and configure CoPP as you would on other Cisco routers running Cisco IOS Software Release 12.4T. The following table summarizes the required steps:

	Command or Action	Purpose

Step 1	**class-map**
	Example:
	`router(config)#class-map match-all TEST-CLASS`
	`router(config-cmap)#match access-group 101`
		Define the packet classification criteria.

Step 2	**policy-map**
	Example:
	`router(config-pmap)#policy-map TEST-POLICY`
	`router(config-pmap)#class TEST-CLASS`
	`router(config-pmap-c)#police rate 12 pps`
		Define the service policy.

Step 3	**control-plane** Example: `router(config)#control-plane`	Access the control plane. **Note** The RPM-XF does not support control plane protection options host, cef-exception, or transit.
Step 4	**service-policy** Example: `router(config-cp)# service-policy input TEST-POLICY`	Apply the service policy.

For more information about control plane policing, refer to the following guides:

- Control Plane Policing [Cisco IOS Software Release 12.4]
- Control Plane Protection [Cisco IOS Software Release 12.4 T]
- Cisco IOS Master Commands List, Release 12.4

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) improves protocol convergence times by rapidly detecting failures in the path between routers. This is especially important for media that does not provide failure signaling, such as Ethernet, because OSPF hello messages can take a second or more to detect the loss. This is too long for some applications and can result in excessive data loss, especially at gigabit rates. BFD quickly detects a media failure so that the OSPF protocol can quickly update routes.

BFD Restrictions

The BFD implementation on the RPM-XF has the following limitations:

- OSPF protocol only
- GIGE interfaces only

BFD Configuration Guidelines

You enable and configure BFD as you would on other Cisco routers running Cisco IOS Software Release 12.4T. BFD is a supporting protocol for OSPF in the RPM-XF, so OSPF must be up and running before BFD can start. The following table summarizes the required steps:

	Command or Action	Purpose
Step 1	**sh ip ospf neighbors** Example: `router# show ip ospf neighbors`	Verify that OSPF neighbors are present and operational.

Step 2	**bfd interval** ***msec*** **min_rx** ***msec*** **multiplier** ***number***
	Example:
	`router(config)# interface GigabitEthernet 1/0`
	`router(config-if)# bfd interval 150 min_rx 150 multiplier 4`
		Configure BFD parameters on interfaces, specifying the interval between sending BFD packets, the interval between receiving BFD packets, and the number of missing BFD packets permitted before declaring a failure.[1]

Step 3	**ip ospf bfd** Example: `router(config-if)# ip ospf bfd`	Enable BFD on interfaces.

	bfd all-interfaces
	Example:
	`router(config)# router ospf 123`
	`router(config-router)# bfd all-interfaces`
		Alternatively, enable BFD globally on all interfaces.

Step 4	**show bfd neighbors** Example `router# show bfd neighbors`	Verify that BFD neighbors are present and that the state is *up*.

1. For configuration restrictions, see CSCsc10658.

BFD Commands

The BFD feature uses the following Cisco IOS commands:

- **bfd all-interfaces**
- **bfd interval**
- **ip ospf bfd**
- **show bfd**

For command reference information, refer to the following document:

- Cisco IOS Master Commands List, Release 12.4

Offline Diagnostics

The RPM-XF already has online hardware and software diagnostics that can test either non-redundant RPM-XF cards or active RPM-XF cards in a redundancy configuration. Release 5.3.00 extends these diagnostic features to the standby card, where they are called offline diagnostics. This improves the availability of the standby card by checking for failures before a switchover.

Similarly, the RPM-XF already has a data-path check that verifies the sanity of the data-path for either non-redundant RPM-XF cards or active RPM-XF cards a redundancy configuration. Release 5.3.00 extends the data-path check to the standby card to test the sanity of its data-path components. This assures that the data path of the standby card is operational and ready to forward traffic if an active card fails.

Offline or online diagnostics run in the following modes:

- User mode—Diagnostic tests are initiated manually.
- Scheduler mode—Diagnostic tests run periodically on a programmable schedule.

Note Only scheduled diagnostics raise alarms and log events.

This section explains how to use both online and offline diagnostics, but Release 5.3.00 introduces offline diagnostics only. For more information about diagnostic commands, refer to New and Modified Commands in Cisco IOS Release 12.4(6)T1, page 23.

Manually Initiating Diagnostics

You can initiate diagnostic tests from the command line as individual tests, tests of a targeted type, or all tests in a test class. A specific test might be an EEPROM cpu diagnostic, a test type might be the fast Ethernet backcard diagnostics, and the test class is either hwdiags or swdiags.

Online diagnostics run on active RPM-PR cards in privileged EXEC mode, and offline diagnostics run on the standby RPM-PR in user EXEC mode. Otherwise, configuration and operational procedures for online and offline diagnostics are the same.

The following table summarizes the required steps to manually initiate online or offline diagnostics:

	Command or Action	Purpose
Step 1	**enable** (active card only)	For online diagnostics, enter the privileged exec mode.
Step 2	**debug rpm [hwdiags | swdiags]** *diag-type* **[***diag-test***]** Offline diagnostic example: `router> debug rpm hwdiags mempool free`	Start the desire tests. Test names and pass/fail results are displayed as they execute. For more information, see debug rpm hwdiags, page 24 and debug rpm swdiags, page 29.

The following example shows how to initiate all mempool offline diagnostics on the standby RPM-XF:

```
Router> debug rpm swdiags mempool free
Mempool Free IO - PASSED
Mempool Free IO - run time = 0 milliseconds
Mempool Free PCI - PASSED
Mempool Free PCI - run time = 0 milliseconds
Mempool Free Processor - PASSED
Mempool Free Processor - run time = 0 milliseconds
```

Scheduling Diagnostics

A scheduler process can periodically run diagnostics tests at a configurable interval. You can schedule individual tests, tests of a functional type, or all tests in a class.

The following table summarizes the required steps to schedule periodic online or offline diagnostics:

	Command or Action	Purpose
Step 1	**enable** (active card only)	For online diagnostics, enter the privileged exec mode.
Step 2	**debug rpm [hwdiags | swdiags]** *diag-type* **[***diag-test***]** **[sched | unsched]** Offline diagnostic example: `router> debug rpm hwdiags cache delay sched`	Schedule the desired diagnostic tests. For more information, see debug rpm hwdiags, page 24 and debug rpm swdiags, page 29.
Step 3	**debug rpm diags display** Offline diagnostic example: `router> debug rpm diags display`	Verify that the scheduler is running. If it is not, start the scheduler. For more information, see debug rpm diags, page 32.

The following example shows how to schedule all software diagnostics:

```
Router> debug rpm swdiags all sched
Mempool Alloc IO - SCHEDULED
Mempool Alloc PCI - SCHEDULED
Mempool Alloc Processor - SCHEDULED
Mempool Free IO - SCHEDULED
Mempool Free PCI - SCHEDULED
Mempool Free Processor - SCHEDULED
Pooltype Packet Header - SCHEDULED
Pooltype Packet Private - SCHEDULED
Pooltype Packet Public - SCHEDULED
Pooltype Particle Private - SCHEDULED
Pooltype Particle Public - SCHEDULED
Corrupt Sprocess - SCHEDULED
Critical Priority Sprocess - SCHEDULED
Dead Sprocess - SCHEDULED
High Priority Sprocess - SCHEDULED
Idle Sprocess - SCHEDULED
Low Priority Sprocess - SCHEDULED
Normal Priority Sprocess - SCHEDULED
```

Starting and Configuring the Scheduler

To perform scheduled diagnostics you must enable the scheduler. Optionally, you can configure the test interval or level of detail for logging (tracelevel). The verbose tracelevel setting is for debugging only.

The following table summarizes the required steps to start and configure the diagnostic scheduler:

	Command or Action	Purpose
Step 1	**enable** (active card only)	For online diagnostics, enter the privileged exec mode.
Step 2	**debug rpm diags cnf enable** Offline diagnostic example: `router> debug rpm diags cnf enable`	Start the scheduler. For more information, see debug rpm diags, page 32.
Step 3	**debug rpm diags cnf** {**period** | **tracelevel**} Offline diagnostic example: `router> debug rpm diags cnf period 60`	Optionally, configure the scheduler period. **Note** The tracelevel option is for troubleshooting only. For more information, see debug rpm diags, page 32.
Step 4	**debug rpm diags display** Offline diagnostic example: `router> debug rpm diags display`	Verify that the scheduler is running. If it is not, start the scheduler. For more information, see debug rpm diags, page 32.

The following example shows how to enable the diagnostic scheduler:

```
Router> debug rpm diags display
Configuration:
    Test: Enabled. Test Interval: 30(secs)
Status:
    Process name:         RPMXF DIAG
    Diag State:           RUN
    Process Error:        No Error
    Last Event Received: ONLN_ENABLE
    Last Event Trigger:   ONLN_ENABLE

Statistics:
    Software Diag runs: 27, failures: 0
    Hardware Diag runs: 49, failures: 0
```

Viewing Results of Scheduled Tests

The following table summarizes the required steps to view and analyze the results of scheduled diagnostic tests:

	Command or Action	Purpose
Step 1	**enable** (active card only)	For online diagnostics, enter the privileged exec mode.
Step 2	**debug rpm [hwdiags | swdiags] stats sched** Offline diagnostic example: `router> debug rpm swdiags stats sched`	Display the results of scheduled tests. For more information, see debug rpm hwdiags stats, page 27 and debug rpm swdiags stats, page 31.
Step 3	**show log** **show facility-alarm status** or from the PXM: **dspcdalms <slot#>** **dsplog**	For tests that fail, determine the reason.

The following example shows how to display the results of scheduled tests:

```
Router> debug rpm swdiags stats sched
Scheduler Software Diag Max Allowed Run Time = 20 milliseconds
Scheduler Software Diag Errors = 0
Scheduler has run 32 Software Diags

Scheduler Software Diags:

ENABLED   Passed           ERR_INJ_OFF    8 millisec  Mempool Alloc IO
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mempool Alloc PCI
ENABLED   Passed           ERR_INJ_OFF    8 millisec  Mempool Alloc Processor
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mempool Free IO
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mempool Free PCI
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mempool Free Processor
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Pooltype Packet Header
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Pooltype Packet Private
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Pooltype Packet Public
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Pooltype Particle Private
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Pooltype Particle Public
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Corrupt Sprocess
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Critical Priority Sprocess
```

```
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Dead Sprocess
ENABLED   Passed           ERR_INJ_OFF    0 millisec  High Priority Sprocess
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Idle Sprocess
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Low Priority Sprocess
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Normal Priority Sprocess
```

Starting and Configuring the Data-Path Check

The data-path check tests the communication link between the active or standby RPM-XF cards and the PXM by periodically transmitting packets and verifying that they are received back correctly. After the maximum retry count when the data-path check is not receiving any packets, the RPM-XF raises an alarm.

You can enable this feature on active and standby RPM-XF cards, but the recovery option (reboot) is not available for the standby card. After a redundancy switchover, the data path check on the standby card is disabled and all the statistics (packets tx/rx) are cleared as the card becomes active.

The following table summarizes the required steps to start and configure the data-path check on the standby card:

	Command or Action	Purpose
Step 1	**cc** *slot* or **ssh**	Establish a management session with the standby RPM-XF.
Step 2	**debug rpm check data-path**	Start the data-path check. For more information, see debug rpm check data-path, page 34.
Step 3	**debug rpm check data-path {interval | retry}**	Configure the data-path check. For more information, see debug rpm check data-path, page 34.

The following table summarizes the required steps to start the data-path check on the active card:

	Command or Action	Purpose
Step 1	**enable**	Enter the privileged exec mode.
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**hw-module rpm check data-path**	Start the data-path check. For more information, see hw-module rpm check data-path, page 33.

Viewing the Data-Path Check Results

The following table summarizes the required steps to view and analyze the results of the data-path check:

	Command or Action	Purpose
Step 1	**cc** *slot* or **ssh**	Establish a management session with the RPM-XF.
Step 2	**show rpm check data-path**	Display the data-path check results. For more information, see show rpm check data-path, page 35.
Step 3	**show log** **show facility-alarm status** or from the PXM: **dspcdalms <slot#>** **dsplog**	For failures, determine the reason.

The following example shows how to display the results of the data-path diagnostic:

```
Router> show rpm check data-path
Data Path Check Health Status:          Good
Data Path Check Feature enabled:        Yes
Data Path Check Recovery enabled:       No
Data Path Check Interval(in sec):       6
Data Path Check Retry Count:            5
Data Path Check Packets Sent:           928
Data Path Check Packets Rcvd:           928
Data Path Check Packets Good:           928
DPC Packets received with Bad header:   0
DPC Packets received with Bad pattern:  0
Data Path Check Outstanding Packets:    1
Data Path Check Time since Last Send:   1
Data Path Check Failures Reported:      0
Data Path Check Recovery Skips Done:    0
Data Path Check Packet Not Sent Reason: None
Data Path Check Packet Sent Wait Time:  0
```

Features Introduced in Cisco IOS Release 12.3(11)T9

No new features were introduced in Cisco IOS Release 12.3(11)T9.

Features Introduced in Cisco IOS Release 12.3(11)T7

No new features were introduced in Cisco IOS Release 12.3(11)T7.

Features Introduced in Cisco IOS Release 12.3(11)T6

No new features were introduced in Cisco IOS Release 12.3(11)T6.

Features Introduced in Cisco IOS Release 12.3(11)T3

Features added to the RPM-XF in Cisco IOS Release 12.3(11)T3 include:

- Copper small-form factor pluggable (SFP)
- RPM-XF software—Queueing elements, statistics, FTP elements, compressed Real-Time Protocol (cRTP) elements, MIBs
- Dynamic bandwidth

For more information, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 5*.

Features Introduced in Cisco IOS Release 12.3(7)T3

Features introduced in Cisco IOS Release 12.3(7)T3 include:

- MGX-XF-UI/B notched back card—A redesign of the user interface back card for the RPM-XF. The notch was 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—Cisco IOS software Release 12.3(7)T3 contains 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 soft permanent virtual connection (SPVC) mastered on that service module. The commands described below are updated to support Preferred Route association through a command-line interface (CLI) or Simple Network Management Protocol (SNMP) for SPVC, Hybrid, and extended permanent virtual connection (XPVC) configured with an RPM-XF as the master end.

Syntax Description

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

Route ID—An identifier for the configured preferred route that is associated with this connection. Preferred routes are maintained 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 sets the connection to be routed only on the specified preferred route. The default value for a directed route is No.

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

 <1 - 65535> Preferred Route ID value

Router(config-if-swconn)# directrte ?

<cr>
```

Note If you use the **directrte** command to specify a directed route for a connection with its preferred route ID set to zero, an error message appears. 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 appears.

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 in Cisco IOS Release 12.3(2)T6

The following new features were introduced in Cisco IOS Release 12.3(2)T6:

- Enhanced Interior Gateway Routing Protocol (eiGRP) between customer edge (CE) to provider edge (PE).
- Basic Point-to-Point Protocol (PPP) over ATM feature evaluation on various port speeds from 768 Kbps up to DS3 with a maximum of T1 bandwidth per flow.
- PPP over ATM with cRTP on various port speeds from 768 Kbps 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 in Cisco IOS Release 12.3(2)T5

No new features were introduced in Cisco IOS Release 12.3(2)T5.

Features Introduced in Cisco IOS Release 12.3(2)T4

This section contains the descriptions of the features that were introduced in 12.3(2)T4.

Link Fragmentation Interleaving

Cisco IOS Release 12.3(2)T4 adds support for Link Fragmentation Interleaving (LFI). For more information on the CLI commands 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*.

For Cisco IOS software configuration informationabout LFI, go to:

- Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtlfifra.htm

Increased Maximum Number of Policy Maps

Policy maps, class maps, and service policy maps define traffic policies, and attach them to interfaces. In earlier releases, you could create 256 separate policy maps and up to 256 class maps per policy map. In Cisco IOS Release 12.3(2)T4, the maximum number of policy maps is 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*.

Multicast VPN Feature

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

For multicast configuration information, go to:

- Multicast VPN—IP Multicast Support for MPLS VPNs

Compressed Real-Time Protocol

The Cisco IOS Release 12.3(2)T4 of the RPM-XF adds the ability to configure the cRTP header.

The CLI commands introduced to support this feature include:

- **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 a match in policy map.

For configuration information, go to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/fthdrcmp.htm

WRED Drop Counters Feature

The WRED Drop Counters feature adds class-based packet counters to existing RPM-XF functionality. The counters can be Differentiated Services Code Point (DSCP) based or precedence based. For more information on the CLI commands introduced or modified to support the weighted random early detection (WRED) Drop Counters feature on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*.

Traffic Matrix Statistics Feature

The Traffic Matrix Statistics (TMS) 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 CLI commands 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*.

Segmentation and Reassembly-based Traffic Management and QoS Feature

Traffic management, weighted random early detection WRED, and cell-based weighted fair queuing algorithm processing is accomplished using the Segmentation and Reassembly (SAR) engine.

Feature Introduced in Cisco IOS Release 12.3(2)T2

This section contains the descriptions of the features that were introduced in 12.3(2)T2.

Transmission Control Protocol Decompression Support

Cisco IOS Release 12.3(2)T2 adds support for Transmission Control Protocol (TCP) decompression as an adjunct to supporting the cRTP header feature on the RPM-XF.

2-Port Packet Over SONET and 2-Port Gigabit Ethernet Service Module Back Cards

Cisco IOS Release 12.3(2)T2 adds support for two service module back cards that provide either two Gigabit Ethernet or two Packet over SONET (POS) ports. For more information on the fit and function of the back cards and CLI commands which support the back cards on the RPM-XF, refer to the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*.

Dual Multiprotocol Label Switching Partition for RPM-XF

Cisco IOS Release 12.3(2)T2 adds support for dual Multiprotocol Label Switching (MPLS) partitions on the RPM-XF. This is related to label switch controller (LSC) redundancy.

For configuration information, go to:

- Preparing RPM Cards for Operation

Features Introduced Earlier than Cisco IOS Release 12.3(2)T2

This section contains the descriptions of the features that were introduced in releases prior to 12.3(2)T2.

Cisco MGX 8950 Switch Support for RPM-XF

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

Border Gateway Protocol Load-Balancing Feature

To load-balance by external Border Gateway Protocol (eBGP) and internal Border Gateway Protocol (iBGP) on multiple paths to a 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 is enhanced to show the multipaths.
	• Each multipath is marked as multipath.
	• The bestpath is marked as multipath and bestpath.
	• The output describes the type of multipath that 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 of eiBGP Load-Balancing

The limitations of eiBGP are as follows:

- If multiple alternate paths for a peering point exist, only one of the paths is used for a given prefix.
- Only per-flow load-balancing is supported. Per-packet load-balancing is not supported.
- eiBGP load-balancing is supported only in MPLS and VPN networks.
- Load-balancing proportional to link bandwidth (see **dmz-linkbw** command) is not supported. The load-balancing is performed on the available links with equal costs.
- The maximum number of paths that can be used for load-balancing is 6. This is the current Cisco IOS software limitation.
- Load-balancing does not work if RDs are the same as RRs. If RRs are used, RDs must be different.
- Having CEs in different VPNs using the same RDs does not work.

IP Accounting Counter Storage Feature

The Cisco MGX RPM-XF only stores packet/byte counters based on precedence and DSCP values on a per-interface level at input.

The following CLIs are 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

The limitations are as follows:

- Counters are maintained only at the input per interface.
- There is no count of dropped or transmitted packets based on DSCP/PREC packets per interface.

Applying Multiple Actions—police Command

The MGX RPM-XF **police** command is similar to the Cisco IOS RPM command. Therefore, you can apply multiple exceed and conform actions on the **police** command.

The **police** CLI command is enhanced. Before 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 allowed only one value for the conform-action and exceed-action fields.

The new **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 you can configure multiple conform-action and exceed-action parameters.

QoS Suboptimal Link Use Feature

RPM-XF uses Versatile Traffic Management System (VTMS) as a scheduling algorithm. VTMS schedules queues based on the current link use 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 use the link.

Cisco IOS Release 12.3(2)T2 adds support through the CLI to allow you to specify the oversubscription factor on a queue. The factor is in the range of 1 through 31 and can be denoted as 2n. An oversubscription factor of n = 2 on any queue means to subscribe that queue by a factor of 4 (2n where n is 2; so 2 raised to power 2 = 4).

The syntax for the **bandwidth** and **priority** commands is:

```
[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. Redundancy that ensures Layer 2 state restoration is supported. Layer 3 state is restored through convergence.

Note When you reset a chassis with RPM-XFs configured for 1:N redundancy, we recommend that you bring up the primary slots in active state.

Benefits of 1:N redundancy include the following:

- 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 performed 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 back cards during front card switchover.
- Y cable redundancy support for POS back cards during front card switchover. With Y cable, 1:N redundancy is restricted to N = 1.

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

- The **Addred** command 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.
- Removing the active RPM-XF back card does not cause a switchover to the standby RPM-XF.
- Before adding redundancy, you must ensure that E:RPM/auto_config_slot# is created. This may require that you log in to the primary card through the command line and manually add **boot config e:auto_config_slot#** followed by a **write mem** command.
- Executing the **switchcc** command back-to-back using the **switchredcd** command can cause problems. We recommend allowing at least 5 seconds between **switchredcd** and a **switchcc**.

- Cisco IOS software on a standby card should be the same or later release than the active RPM-XF card release.
- If the card is in a redundancy group, do not boot the card from an image on a TFTP server. Boot the card from image in bootflash or PXM disk only.
- Do not configure the standby RPM-XF.

Features Not Supported in Cisco IOS Release 12.3(11)T7

The following features are not supported in Cisco IOS Release 12.3(11)T5:

- LSC redundancy
- Modem connectivity on auxiliary port
- MPLS TE tunnels on ATM interfaces
- Online insertion and removal (OIR) of back cards without interfaces in shutdown mode
- Per-packet load-balancing
- ROM monitor (ROMmon) Xmodem functionality does not support the speed option
- RPM-PR to RPM-XF upgrade
- Virtual circuit (VC) merge

Network Management Features

Network management features are detailed in the *Release Notes for Cisco WAN Manager 15.1.50* at:

- http://cisco.com/univercd/cc/td/doc/product/wanbu/svplus/151/rnotes/index.htm

SNMP MIB

MGX Release 5.2.00 SNMP MIB files are provided in Cisco IOS Release 12.3(11)T7. These files can be compiled with most standards-based MIB compilers. The tar file contains the MGX MIB files and the MIB release notes.

Cisco IOS MIBs are not part of the MGX Release 5.2.00 SNMP MIB bundle; they are part of Cisco IOS Release 12.3(11)T7.

New and Modified Commands in Cisco IOS Release 12.4(6)T1

The following commands, not previously documented, are modified in Cisco IOS Release 12.4(6)T1:

- debug rpm hwdiags
- debug rpm hwdiags stats
- debug rpm swdiags
- debug rpm swdiags stats
- debug rpm diags

- hw-module rpm check data-path
- debug rpm check data-path
- show rpm check data-path

Cisco IOS Release 12.4(6)T1 introduces the following new commands:

- hw-module rpm pxm-tod-ignore (CSCsc20181)
- hw-module pxf cef-mem-threshold (CSCei95224)
- atm sar-buffers tx (See SAR Enhancements, page 7)

debug rpm hwdiags

To perform online or offline diagnostics on RPM-XF hardware, use the **debug rpm hwdiags** command.

debug rpm hwdiags *diag-type* [*diag-test*] [**clrerr | injerr | info**] [**sched | unsched**]

Syntax Description

diag-type	The type of tests to run or schedule: • **all**—All hardware diagnostics • **atmdx**—ATMDX hardware diagnostics • **POS**—One-port POS • **2POS**—Two-port POS • **cache**—Cache hardware • **cbc**—CBC hardware • **dge**—2-Port Gigabit Ethernet • **eeprom**—EEPROM hardware • **flash**—Flash hardware • **ge**—One-port Gigabit Ethernet • **iofpga**—IO FPGA hardware • **memory**—Memory hardware • **nvram**—NVRAM hardware • **pci**—PCI hardware • **swbarium**—Switch barium hardware

diag-test	The specific test to run or schedule: • ATMDX tests – **cbc-id**—CBC SAR device/vendor ID hardware diagnostics – **rxsar-id—**ATMDX RX SAR device/vendor ID hardware diagnostic – **txsar-id—**ATMDX TX SAR device/vendor ID hardware diagnostic • POS tests – **barium**—Backcard BARIUM hardware diagnostic – **fib**—Backcard FIB hardware diagnostic – **posio**—Backcard POSIO hardware diagnostic – **sky**—Backcard SKY hardware diagnostic – **tib**—Backcard TIB hardware diagnostic • 2POS tests – **dpio**—Backcard DPIO hardware diagnostic – **eeprom**—Backcard EEPROM hardware diagnostic – **pm5358**—Backcard PM5358 asic hardware diagnostic – **vanadium**—Backcard vanadium hardware diagnostic • cache tests – **delay**—Delay cache hardware diagnostic – **l1-size**—L1 size cache hardware diagnostic • cbc tests – **reg**—CBC register hardware diagnostic • dge tests – **dpio**—Backcard DPIO hardware diagnostic – **eeprom**—Backcard EEPROM hardware diagnostic – **pm3386**—Backcard PM5358 asic hardware diagnostic – **vanadium**—Backcard vanadium hardware diagnostic • eeprom tests – **cpu—**EEPROM CPU hardware diagnostic • flash tests – **access—**Flash access hardware diagnostic (active card only) – **device—**Flash device hardware diagnostic

diag-test (continued)	• ge tests – **barium—**Backcard BARIUM hardware diagnostic – **cam—**Backcard CAM hardware diagnostic – **fib—**Backcard FIB hardware diagnostic – **gigmac—**Backcard GIGMAC hardware diagnostic – **posio—**Backcard POSIO hardware diagnostic – **tib—**Backcard TIB hardware diagnostic • iofpga test – **reg—**IO FPGA register hardware diagnostic • memory tests – **busfloat32—**32-bit word memory diagnostic – **busfloat32-delay—**32-bit word delay memory diagnostic – **cache-pattern—**Memory cache pattern diagnostic – **delay—**Memory delay diagnostic – **marching-pattern—**32-bit marching pattern memory diagnostic – **marching-pattern-delay—**32-bit marching pattern delay memory diagnostic – **r4k-access—** R4K memory access diagnostic • nvram tests – **data-pins—**Nvram data pins hardware diagnostic – **march—**Nvram marching data pattern hardware diagnostic pci tests • PCI tests – **bridge—**PCI bridge hardware diagnostic – **id—**PCI ID hardware diagnostic • swbarium tests – **reg—**Switch barium register hardware diagnostic
clrerr	Turn the error injection off.
injerr	Turn the error injection on.
info	Display a description of the test.
sched	Schedule a diagnostic test.
unsched	Cancel a scheduled test.

Command Default None.

Command Modes Privileged EXEC for online diagnostics; User EXEC for offline diagnostics.

Command History

Release	Modification
12.4(6)T1	This command was extended to offline diagnostics

Usage Guidelines

Use this command to initiate hardware diagnostics or select diagnostics for periodic execution. You enter the **sched/unsched** keywords to select or deselect diagnostics for periodic execution.

If you enter **all** as the *diag-type*, then all hardware tests are executed. If you specify the *diag-type* without the optional *diag-test* parameter, then all *diag-test*s within in the *diag-type* execute, for example all POS backcard tests. If you specify the *diag-test*, then only the specified *diag-test* executes.

Examples

The following example shows how to run all nvram diagnostics on the standby card:

```
Router> debug rpm hwdiags nvram
NVRAM Data Pins - PASSED
NVRAM Data Pins - run time = 0 milliseconds
NVRAM Marching Pattern - PASSED
NVRAM Marching Pattern - run time = 0 milliseconds
```

The following example shows how to schedule all nvram diagnostics on the standby card:

```
Router> debug rpm hwdiags nvram sched
NVRAM Data Pins - SCHEDULED
NVRAM Marching Pattern - SCHEDULED
```

Related Commands

Command	Description
debug rpm swdiags	Perform RPM software diagnostics.
debug rpm check data-path	Perform RPM data-path diagnostic.

debug rpm hwdiags stats

To display or clear the results of hardware diagnostics and to configure the maximum scheduled diagnostics time, use the **debug rpm hwdiags stats** command.

debug rpm hwdiags stats {sched | boot | clear | maxtime}

Syntax Description

sched	Display the results of scheduled hardware diagnostics.
boot	Display the results of boot diagnostics.
clear	Clear the statistics.
maxtime	Set the maximum run time for hardware diagnostics.

Command Default

None

Command Modes

Privileged EXEC for online diagnostics; User EXEC for offline diagnostics.

Command History

Release	Modification
12.4(6)T1	This command was extended to offline diagnostics

Usage Guidelines

Use this command to clear or display the results of hardware diagnostics, and to configure the maximum scheduled diagnostics time.

Examples

The following example shows how to display the results of scheduled hardware diagnostics:

```
Router> debug rpm hwdiags stats sched
Scheduler Hardware Diag Max Allowed Run Time = 20 milliseconds
Scheduler Hardware Diag Errors = 0
Scheduler has run 64 Hardware Diags

Scheduler Hardware Diags:

ENABLED   Passed           ERR_INJ_OFF    4 millisec  Cache Delay
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Cache L1 Size
ENABLED   Passed           ERR_INJ_OFF    8 millisec  EEPROM Cpu
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mxt4700 RX SAR Device/Vendor Id
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mxt4700 TX SAR Device/Vendor Id
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Mxt4400 CBC SAR Device/Vendor Id
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Flash Device
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory Bus Float 32
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory Bus Float 32 with Delay
ENABLED   Passed           ERR_INJ_OFF    8 millisec  Memory Cache Pattern
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory Delay
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory Marching Pattern
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory Marching Pattern with Delay
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Memory R7K Access
ENABLED   Passed           ERR_INJ_OFF    0 millisec  IO FPGA Reg
ENABLED   Passed           ERR_INJ_OFF    0 millisec  NVRAM Data Pins
ENABLED   Passed           ERR_INJ_OFF    0 millisec  NVRAM Marching Pattern
ENABLED   Passed           ERR_INJ_OFF    0 millisec  PCI Bridge
ENABLED   Passed           ERR_INJ_OFF    0 millisec  PCI ID
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Frontcard BARIUM Reg
ENABLED   Passed           ERR_INJ_OFF    0 millisec  CBC Reg
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Backcard VANADIUM Reg
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Backcard DPIO Reg
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Backcard EEPROM
ENABLED   Passed           ERR_INJ_OFF    0 millisec  Backcard PM5358 Reg
```

Related Commands

Command	Description
debug rpm swdiags stats	Display the results of scheduled software diagnostics.
debug rpm swdiags	Perform RPM software diagnostics.

debug rpm swdiags

To perform online or offline diagnostics on RPM-XF software, use the **debug rpm hwdiags** command.

debug rpm swdiags *diag-type* [*diag-test*] [**clrerr | injerr | info**] [**sched | unsched**]

Syntax Description

diag-type	The type of tests to run or schedule: • **all**—All Software diagnostics • **mempool**—Mempool software • **pooltype**—Pooltype software • **sprocess**—Sprocess software
diag-test	The specific test to run or schedule: • mempool tests – **alloc**—Alloc mempool diagnostics **io**—IO memory test **pci**— PCI memory test **processor**—Processor memory test – **free**—Free mempool diagnostics **io**—IO memory test **pci**— PCI memory test **processor**—Processor memory test • pooltype tests – **packet**—Packet pooltype diagnostics **header**—Packet header test **private**—Private packet pooltype test **public**—Public packet pooltype test – **particle**—Particle pooltype diagnostics **private**—Private particle pooltype test **public**—Public particle pooltype test
diag-test (continued)	• sprocess tests – **corrupt**—Corrupt Sprocess software diagnostic – **critical**—Critical priority Sprocess software diagnostic – **dead**—Dead Sprocess software diagnostic – **high**—High priority Sprocess software diagnostic – **idle**—Idle Sprocess software diagnostic – **low**—Low priority Sprocess software diagnostic – **normal**—Normal priority Sprocess software diagnostic
clrerr	Turn the error injection off.

injerr	Turn the error injection on.
info	Display diagnostic description.
sched	Display a description of the test.
unsched	Schedule a diagnostic test.

Command Default

No defaults.

Command Modes

Privileged EXEC for online diagnostics; User EXEC for offline diagnostics.

Command History

Release	Modification
12.4(6)T1	This command was extended for offline diagnostics

Usage Guidelines

Use this command to initiate software diagnostics or select diagnostics for periodic execution. You enter the **sched/unsched** keywords to select or deselect diagnostics for periodic execution.

If you enter **all** as the *diag-type*, then all hardware tests are executed. If you specify the *diag-type* without the optional *diag-test* parameter, then all *diag-test*s within in the *diag-type* execute, for example all mpool tests. If you specify the *diag-test*, then only the specified *diag-test* executes.

Examples

The following example shows how to test the free memory pool on the standby card:

```
Router> debug rpm swdiags mempool free
Mempool Free IO - PASSED
Mempool Free IO - run time = 0 milliseconds
Mempool Free PCI - PASSED
Mempool Free PCI - run time = 0 milliseconds
Mempool Free Processor - PASSED
Mempool Free Processor - run time = 0 milliseconds
```

The following example shows how to schedule the free memory pool diagnostic on the standby card:

```
Router> debug rpm swdiags mempool free sched
Mempool Free IO - SCHEDULED
Mempool Free PCI - SCHEDULED
Mempool Free Processor - SCHEDULED
```

Related Commands

Command	Description
debug rpm hwdiags	Perform RPM hardware diagnostics.
debug rpm check data-path	Perform RPM data-path diagnostic.

debug rpm swdiags stats

To display or clear the results of software diagnostics, use the **debug rpm swdiags stats** command.

debug rpm hwdiags stats {sched | clear | maxtime}

Syntax Description

sched	Display the results of scheduled software diagnostics.
clear	Clear the statistics.
maxtime	Set the maximum run time for software diagnostics.

Command Default

None

Command Modes

Privileged EXEC for online diagnostics; User EXEC for offline diagnostics.

Command History

Release	Modification
12.4(6)T1	This command was extended to offline diagnostics

Usage Guidelines

Use this command to display the results of software diagnostics, or to clear the results.

Examples

The following example shows how to display the results of software diagnostics:

```
Router> debug rpm swdiags stats sched
Scheduler Software Diag Max Allowed Run Time = 20 milliseconds
Scheduler Software Diag Errors = 0
Scheduler has run 52 Software Diags

Scheduler Software Diags:

ENABLED   Passed            ERR_INJ_OFF    8 millisec  Mempool Alloc IO
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Mempool Alloc PCI
ENABLED   Passed            ERR_INJ_OFF    8 millisec  Mempool Alloc Processor
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Mempool Free IO
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Mempool Free PCI
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Mempool Free Processor
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Pooltype Packet Header
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Pooltype Packet Private
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Pooltype Packet Public
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Pooltype Particle Private
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Pooltype Particle Public
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Corrupt Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Critical Priority Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Dead Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  High Priority Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Idle Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Low Priority Sprocess
ENABLED   Passed            ERR_INJ_OFF    0 millisec  Normal Priority Sprocess
```

Related Commands

Command	Description
debug rpm hwdiags stats	Display the results of scheduled hardware diagnostics.
debug rpm hwdiags	Perform RPM hardware diagnostics.

debug rpm diags

To enable the diagnostic scheduler and configure the test interval, use the **debug rpm diags** command. To disable the scheduler, use the **no** form of this command.

debug rpm diags cnf {**enable** | **period** *sec* | **tracelevel** *level*}

debug rpm diags display

no debug rpm diags cnf enable | tracelevel

Syntax Description

enable	Enable the scheduler
period	Scheduler period in seconds. Default: 30 seconds
tracelevel	Trace level: • 1—brief trace • 2—normal trace • 3—verbose trace **Note** The tracelevel option is for troubleshooting only. Do not change for normal operation.
display	Display scheduler information.

Command Default

No defaults.

Command Modes

Privileged EXEC for online diagnostics; User EXEC for offline diagnostics.

Command History

Release	Modification
12.4(6)T1	This command was extended for offline diagnostics

Usage Guidelines

Use this command to enable the diagnostic scheduler or configure scheduler parameters. The scheduler executes the tests previously selected with the **debug rpm hwdiags** or **debug rpm swdiags** commands.

Examples

The following example enables the diagnostic scheduler:

```
Router> debug rpm diags cnf enable
Router> debug rpm diags display
Configuration:
    Test: Enabled. Test Interval: 30(secs)
Status:
    Process name:         RPMXF DIAG
    Diag State:           RUN
    Process Error:        No Error
    Last Event Received: ONLN_ENABLE
    Last Event Trigger:  ONLN_ENABLE

Statistics:
    Software Diag runs: 9, failures: 0
    Hardware Diag runs: 4, failures: 0
```

Related Commands

Command	Description
debug rpm hwdiags	Perform RPM hardware diagnostics.
debug rpm swdiags	Perform RPM software diagnostics.

hw-module rpm check data-path

To enable the data path check on the active RPM-XF card, use the **hw-module rpm check data-path** command in the global configuration mode. To disable the data-path check, use the **no** form of this command.

hw-module rpm check data-path [**interval** *sec* | **retry** *num* | **recovery**]

no hw-module rpm check data-path

Syntax Description

interval	The interval between successive packets, in seconds.
retry	The number of retries.
recovery	Turn on/off the recover option.

Command Default

No defaults.

Command Modes

Global configuration mode

Usage Guidelines

Use this command to enable the data-path diagnostic on the active RPM-XF.

Examples The following example enables the data-path diagnostic:

```
Router<config># hw-module rpm check data-path
```

Related Commands

Command	Description
debug rpm check data-path	Enable the data-path check on the standby RPM-XF.
show rpm check data-path	Display data-path check results.

debug rpm check data-path

To enable the data path check on the standby RPM-XF card, use the **debug rpm check data-path** command in the user EXEC mode. To disable the data-path check, use the **no** form of this command.

debug rpm check data-path [**interval** *time* | **retry** *num*]

no debug rpm check data-path

Syntax Description

interval	The interval between successive packets, in seconds. Default: 6 sec
retry	The maximum number of retries. Default: 5 retries

Command Default No defaults.

Command Modes User EXEC

Command History

Release	Modification
12.4(6)T1	This command was introduced.

Usage Guidelines Use this command to enable the data-path diagnostic or to configure test parameters on the standby card. To disable the debug tests on the standby card, you can enter **no debug rpm** or **undebug**.

Examples The following example enables the data-path check:

```
Router> debug rpm check data-path
```

Related Commands

Command	Description
hw-module rpm check data-path	Enable the data-path check on the active RPM-XF.
show rpm check data-path	Display data-path check results.

show rpm check data-path

To display the data-path check information on the standby RPM router, use the **show rpm check data-path** command in user EXEC mode.

show rpm check data-path

Command Default

No defaults.

Command Modes

User EXEC mode.

Command History

Release	Modification
12.4(6)T1	This command was extended for offline diagnostics

Usage Guidelines

Use this command to display data-path diagnostic results.

Examples

The following example shows data-path results on the standby card:

```
Router> show rpm check data-path
Data Path Check Health Status:          Good
Data Path Check Feature enabled:        Yes
Data Path Check Recovery enabled:       No
Data Path Check Interval(in sec):       6
Data Path Check Retry Count:            5
Data Path Check Packets Sent:           11994
Data Path Check Packets Rcvd:           11993
Data Path Check Outstanding Packets:    1
Data Path Check Time since Last Send:   1
Data Path Check Failures Reported:      0
Data Path Check Recovery Skips Done:    0
Data Path Check Packet Not Sent Reason: None
Data Path Check Packet Sent Wait Time:  0
```

Related Commands

Command	Description
debug rpm check data-path	Enable the data-path check on the active RPM-XF.
hw-module rpm check data-path	Enable the data-path check on the active RPM-XF.

hw-module rpm pxm-tod-ignore

To ignore the time of day update from the PXM, use the **hw-module rpm pxm-tod-ignore** command in global configuration mode. To use the time of day update from the PXM, use the **no** form of this command.

hw-module rpm pxm-tod-ignore

no hw-module rpm pxm-tod-ignore

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
12.4(6)T1	This command was introduced.

Usage Guidelines

By default, the RPM-XF updates its clock to the time of day (TOD) sent by the PXM. If the RPM-XF is synchronized to an Network Time Protocol (NTP) server, the TOD update from PXM might make the RPM-XF go out of sync with the NTP server. Use this command when using NTP to configure the RPM-XF to ignore the TOD update from the PXM.

Examples

The following example <<text>>:

```
Router(config)#hw-module rpm pxm-tod-ignore
```

Related Commands

Command	Description
none	none

hw-module pxf cef-mem-threshold

To set a warning threshold for Cisco Express Forwarding (CEF) memory, use the **hw-module pxf cef-mem-threshold** command in global configuration mode. To disable this warning, use the **no** form of this command.

hw-module pxf cef-mem-threshold *percent*

no hw-module pxf cef-mem-threshold *percent*

Syntax Description

percent	Percent of memory usage of type 1 to 12 for which a warning is issued. Range: 1to 99

Command Default

No defaults

Command Modes

Global configuration mode

Command History

Release	Modification
12.4(6)T1	This command was introduced.

Usage Guidelines

This command sets a threshold and enables a warning message if any PXF CEF queue exceeds the specified threshold. Use the **show pxf cpu cef** command to display memory types 1 to 12.

Examples

The following example sets the memory threshold to 10%:

```
hw-module pxf cef-mem-threshold 10
```

Related Commands

Command	Description
show pxf cpu cef	Displays the PXF memory usage of the current Cisco Express Forwarding (CEF) table.

atm sar-buffers tx

To manually set the size of the UBR, VBR and LVC buffers, use the **atm sar-buffers tx** command in interface configuration mode. To restore default buffer allocations, use the **no** form of this command.

atm sar-buffers tx *UBR VBR LVC*

no atm sar-buffers tx

Syntax Description

UBR	The buffer size for UBR. Range: 2048-339968 Default: 86016
VBR	The buffer size for VBR. Minimum: 2048 Maximum: Depends on UBR value Default: 172032
LVC	The buffer size for LVC. Value: Depends on UBR and VBR values Default: 86016

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
12/4(6)T1	This command was introduced.

Usage Guidelines

You use the **atm sar-buffers tx** command to reallocate the total SAR buffers between UBR, VBR and the LVC classes based on expected usage for these traffic classes. Use the show controllers Switch1 command to monitor the buffers allocated for each class, the actual buffer usage for each class, and the cumulative queue sizes of all VCs in each class. Class 1 is UBR, Class 2 is VBR & Class 3 is LVC.

Examples

The following example sets the UBR, VBR, and LVC buffer sizes to 2048, 339968, 2048, respectively.

```
atm sar-buffers tx 2048 339968 2048
```

Related Commands

Command	Description
show controllers switch1	Display controller information for the interface switch1.

RPM-XF Limitations and Restrictions

The following RPM-XF limitations and restrictions apply to this release:

- Before you add redundancy, you must create E: RPM/auto_config_slot#. This may require a login through the CLI and manually adding the **boot config** command followed by a **write mem** command.
- Permanent Virtual Paths (PVPs) cannot operate at a rate greater than 599,039 kbps.
- PXF buffer depletion may occur if packets of the same size (especially packets greater than 640 bytes) are sent to a congested interface.
- High speed VC Sustainable Cell Rate (SCR) greater than or equal to 599,039 kbps does not receive full-configured rate for single flow (unique source and destination IP address). This happens because for high speed VCs, Parallel Express Forwarding (PXF) creates two queues and these queues cannot be shared for the same stream. Sharing two queues for the same stream causes out–of–sequence packets.
- The PXF queue selection algorithm may cause traffic to drop for multiple streams traveling to the same destination using multiple paths. When the PXF receives 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 multiple paths for the same destination exist, multiple streams may possibly hash to one queue, causing some queues to overflow, while others might be underused.
- Variable bit rate non-real time (VBR-nrt) and variable bit rate-real time (VBR-rt) are treated with the same priority system-wide.
- RPM-XF PVP only supports unspecified bit rate (UBR).
- PVP in RPM-XF is not Operation, Administration, and Maintenance (OAM) managed.
- If out-of-sync SPVC or SPVP exist on the RPM-XF, the shrinking of the Private Network-to-Network (PNNI) partition is not permitted.
- One RPM-XF can serve as either an edge Label Switch Router (eLSR) or as an LSC, but not as both.
- Because RPM-XF only supports UBR, VBR-rt, and VBR-nrt on the PXM, the **dsppnportrsrc** command for RPM-XF port shows 0 available resources for CBR, ABR, and signaling service types. Also, the **cnfpnportcac** command for CBR and ABR is rejected.
- If RPM-XF is configured as an eLSR, RPM-XF does not support incoming VC-merge label switch controlled virtual circuits (LVCs). There is a problem logged against LSC module that it cannot support both VC-merge/non-VC-merge supporting Virtual Switch Interface (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 up to two MPLS subinterfaces. If you attempt to configure over the limit, an error message appears.
- Although RPM-XF VSI slave supports the connections statistics **get** command, only packet and byte counts are available. Therefore, use the **show xtag cross-connect traffic int xtagatm** command connection statistic to show how on the LSC module, packet counts from RPM-XF eLSR exist.
- OIR of MGX-1GE and MGX-1OC-12POS-IR back cards are supported only with interfaces in shutdown state.
- The MGX-1GE back card does not have the capability to provide line loopback.
- The Flow Control option is not configurable with the MGX-1GE back card.
- The MGX-1GE back card does not support SFP security.

- Line loopback and internal loopback cannot be set at the same time for the MGX-1OC-12POS-IR back card using AMCC Mux.
- The **pos ais-shut** command is not supported on MGX-1OC-12POS-IR back card.
- The traffic rate per flow is at half the interface speed for POS Gigabit Ethernet interfaces in this release.
- When traffic is traveling on Gigabit Ethernet interfaces, do not toggle autonegotiation. This may result in permanent disruption of traffic.
- For UBR, two queues always exist which results in half the flow rate for each flow because the hashing algorithm hashes the two into one queue.

The performance limits supported in Release 5.2.00 include the following:

- 2K ATM SPVC connection endpoints
- 2K Interface Description Blocks (IDBs)
- 4K LVCs
- 100 Virtual Path Connections (VPCs)
- 2048 policy map
- 100 open shortest path first (OSPF) neighbors
- 6 Cisco IOS-based cards in the Cisco MGX chassis
- 500 VPN routing/forwarding instances (VRFs)
- 500 BGP CE peers
- 100 Routing Information Protocol (RIP) CE sessions
- 500 Static CEs
- 100,000 VPN Routes per PE
- 250K non-VPN Routes per RPM-XF
- 300 OAM-enabled connections
- mVPN limits
  - 384 mVRF
  - 64K Mroutes
  - 256K outgoing interfaces for Mroutes

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

Notes and Cautions

Before you use this release, review the following notes and cautions:

- When removing the SFP-GE-T transceiver module from the MGX-XF Back Card, pull the bale out and down to fully open (unlocked) position to eject the SFP transceiver from the socket connector. Then, grasp the SFP transceiver between your thumb and index finger, and carefully remove it from the socket.

  If the SFP transceiver appears to be stuck, with the SFP latch in the fully unlocked position, push it back into the socket to release the latch, then pull out to remove it.

Caution DO NOT use a screwdriver to pry the SFP transceiver loose! This will damage the socket on the MGX-XF Back Card.

- 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** command 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, this is when you may see the card 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.
- When you execute a **dspcds** command, a new stable boot-hold state appears on the PXM45. This state indicates that the RPM-XF is running only a boot image. This state is reached when the config register is set to 0x1 or when the bootldr cannot find the run-time image, but finds the boot image. Enter the **cc** command to access the RPM-XF from the PXM45.
- A valid boot image need not be the first file in the bootflash. The RPM-XF loads from any valid boot image from the **bootflash:**. The run-time image can be the first file in the bootflash flash and RPM-XF comes up with that image.
- Trying to change peak cell rate (PCR) value of a VP tunnel or changing the maximum transmission unit (MTU) of switch interface with more than 4000 VCs may overuse the CPU.
- If a large number of VCs (PVCs, LVCs or both) exist on the RPM-XF card and are executing disruptive operations on the main switch interface (int switch1), this may cause flapping of the protocols that run on these VCs. Examples of disruptive operations are **clear int switch1** and modification of PVP parameters. These operations cause deactivation and reactivation of all VCs under the main switch interface. Depending on the number of VCs, the time required to complete such operations may exceed a certain protocol timeout limit. Examples of protocols that may be affected are OSPF and Tag Distribution Protocol (TDP)/Label Distribution Protocol (LDP).
- The RPM-XF VSI slave tends to put out informational warning/traceback messages caused by misconfigurations and connection admission control (CAC) failures (onto console/IOS log file). These messages are for information and debugging purposes. 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 the Cisco IOS *pvc* CLI may not be the same as the SCR programmed in the PXF. PXF bandwidth chunk size is 18 kbps. All PXF VC SCRs are programmed as multiples of 18 kbps. For instance, if the PVCs were configured with 50 kbps as PCR, 54 kbps are programmed in PXF. The **show atm pvc** commands shows 50 kbps, and the VSI slave accounts 50 kbps during CAC. However, 54 kbps is being used. As a result, when bandwidth use reaches the maximum value, both the VSI slave and the PNNI continue to allow connection provisioning, because the VSI slave and the PNNI available bandwidth show more than the PXF has remaining.
- The **saveallcnf** command (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 before you enter the **saveallcnf** command. This also ensures that the RPM-XF files on the active PXM45 hard disk contain the latest configuration to be saved.
- For eLSR to LSC connectivity, use the default control VC of 32. If a 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 the control VC from any VCI value within the range defined in the partition. The same VC should be defined on the LSC on the Xtag interface.
  - Reconfigure the PNNI partition to spare the control VC usage on the RPM-XF and AXSM, AXSM/B or AXSM-E APS Management Information.
- Each time you change the RPM-XF configuration, enter the **write mem** command on the RPM-XF to save the configuration. If you do not do this, the changed configuration is 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. Set the *slot#* portion of the name 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 nonvolatile RAM (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 the 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, the NVRAM version is used.

Note In case of RPM-XF redundancy, store the configuration in the *auto_config_slot#* file in the E:RPM directory of the PXM45 hard disk. Failure to find the autoconfig file causes a user-initiated switchover (**switchredcd**) to abort and a fatal error is flagged.

Card Management

Before you use Release 12.3(11)T7, review the following card management notes and cautions:

- 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 displays as *boot*>.
- The run-time Cisco IOS image cannot be used as a bootloader to load a different Cisco IOS image.
- Changing the 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 0x2102.

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

Note We recommend you always use 9600 baud as the console speed.

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

Note The **loadrev** and **setrev** commands 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 prevents the card from booting.

The RPM-XF boot image, which is shipped loaded on the flash, works for all RPM-XF Cisco IOS images; therefore, there is no reason to delete or move the factory installed boot image.

To avoid unnecessary failures that require card servicing, remember 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.

If the boot file remains intact in the first position on the flash, the RPM-XF boots successfully.

If the bootflash is corrupt, use the **tftpdnld** command described in the *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide* or the xmodem procedure described in the "Using XModem to Download Flash to RPM-XF Cards" section on page 66 to download a new boot image.

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

If you add more than 11 VISM cards to an MGX chassis with RPM-XF cards, this requires that you enable the expanded memory option on the PXM45/B. The command to enable this option is **cnfndparms** (option 4). This expanded memory option does not have an impact on chassis performance and allows more connections.

Open Caveats

This section contains the open caveats in Cisco IOS Releases 12.4.x and 12.3.x.

Open Caveats in Cisco IOS Release 12.4(6)T1

Table 1 lists caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00.

Table 1 Open Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00

Caveat Number	Symptom	Conditions	Workaround
CSCee72462	Class queue size is programmed incorrectly for WRED queues.	RPM-XF has PXF-based QoS, WRED is configured for the class queue.	**shutdown/no shutdown** on the interface or removal/addition of the service policy can resolve the error in certain cases.
CSCef75810	Traceback encountered on RPM-XF.	Create a switch sub interface and associate it to a bridge group.	None. This traceback does not have any service impact.

Table 1 Open Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCin98686	A redundant pair of RPM-XF cards fail after **show startup-config** on the primary RPM-XF when the auto_config_slot<slot_no> file is deleted.	Redundancy pair of RPM-XF cards.	None
CSCsb07616	**debug rpm check-image now** <*image-name*> on an RPM-XF card might fail.	Memory fragmentation on RPM-XF due to high memory usage.	None
CSCsb91110	Policy map does not display per-dscp wred counters in **show policy-map interface** Switch1.xx	The per-dscp wred counters are not displayed only when multicast traffic is being sent on high speed RPM-XF. Unicast traffic does not exhibit this problem.	Use the match statistics under the policy map for dscp stats.
CSCsb91157	The policy map output queue shows a different number of packets than the match statistics displayed under a particular class in **show policy-map interface** Sw1.xx.	This issue is observed when using high speed RPM-XF and multicast traffic. Unicast traffic does not exhibit the issue.	Use Interface and PVC statistics for more accurate information.
CSCsc05844	Interface missing in hardware mroute after **shutdown/no shutdown** of interface.	The outgoing interface is a static IGMP join and a **shutdown/no shutdown** is done on that interface.	**clear ip mroute vrf** <> <*mroute*>
CSCsc10658	BFD sessions flap on a Cisco RPM-XF Router.	The following BFD aggressive timers are configured: bfd interval 50 min_rx 50 multiplier 3 And the following operations are performed: (1) Enter **no boot system** or **no boot system image** any time (2) Enter **write memory** for the first time after changing boot variables such as boot system, boot config, or boot bootldr.	The aggressive timers can be safely used if the stated operations are done only during maintenance. Instead, use **bfd interval 150 min_rx 150 multiplier 4** to avoid BFD session flaps,
CSCsc34793	The following counter increments without bounds periodically in the **show pxf dma counters** PXF DMA FBB Line Card Error PXF DMA Toaster Status Wait Error PXF DMA TTQ Context Wait Error	This occurs when there is a Cobalt event that triggers any of the errors listed in symptoms. Even without more Cobalt events, the error counters increment.	None

Table 1 Open Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCsc84768	BFD configuration under Ethernet type of interfaces is lost.	After the removal / insertion of the Ethernet type of interface.	None
CSCsc84791	**show interface switch** 1 displays incorrect input error counter values.	After clearing the toaster statistics using **clear pxf statistics**.	None
CSCsc92289	Unable to correctly determine if UDP compression is enabled or disabled on RPM-XF.	**sh rpm udp-comp** is executed to determine if the feature to turn off UDP compression is enabled or disabled.	None
CSCsd30108	RPM-XFL card is not passing any traffic and control plane protocols are down.	Data path segmentation SAR shows buffer exhaustion, and multi-bit ECC error observed.	None
CSCsd34529	The Cisco RPM-XF router crashes when simultaneous display and unconfiguring of policy maps is taking place.	The Cisco RPM-XF Router is running a 12.4T image. **no policy-map** <*name*> is executed on a CLI session. **show policy-map** is executed on another CLI session.	None
CSCsd66607	In eiBGP multipath loadbalancing, PXF does not display rewrite string value for MPLS path, but traffic flow and loadbalancing is not affected.	In eiBGP multipath loadbalancing scenario, **show pxf cpu cef vrf** <*vrf#*> <*prefix*> displays rewrite string for IP path, but not for MPLS path.	None

Table 1 Open Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCsd68085	RPM-XF card goes to ROMMON state when typing on the console port. The console port and term server port have a speed mis-match.	RPM-XF Console port and Term server Async port have a mismatch. On the RPM-XF console the receive speed is in mismatch with the other end transmit speed of the other end. BREAK is enabled on the RPM-XF (in the config-register setting) Occurs with all RPM-XF images	There are two possible workarounds 1.Disable BREAK (in the config-register setting) The config-register is a 16 bit entity with the following 4 nibble representation xxxx xxxy xxxx xxxx ===> 16 bits Set the 'y' bit to 1 to disable BREAK 2. If BREAK is not disabled, do not type on the console after the speed mismatch occurs. Make sure that the speed mismatch is corrected before typing on the console. It is feasible to use "cc" or "telnet" under these conditions without using the console
CSCsd70876	When multiple iBGP paths are available, PXF chooses one of the iBGP paths. Sometimes the PXF-chosen iBGP path is different than the IOS-chosen iBGP path.	With multiple iBGP paths available, verify the iBGP path chosen by IOS and PXF using following commands: **show ip cef vrf** <*vrf#*> <*prefix*> **show pxf cpu cef vrf** <*vrf#*> <*prefix*>	None

Open Caveats in Release 12.3(11)T9

Table 2 lists caveats in Cisco IOS Release 12.3(11)T9 for MGX Release 5.2.10.

Table 2 Open Caveats in Cisco IOS Release 12.3(11)T9 for MGX Release 5.2.10

Caveat Number	Symptom	Conditions	Workaround
CSCin97913	The output of **show rpm card** command displays Auto configuration file used as none.	Under normal conditions without redundancy even though the boot config file is set and auto config file is in PXM.	None

Table 2 Open Caveats in Cisco IOS Release 12.3(11)T9 for MGX Release 5.2.10 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCin98465	The **show int gig1/0** shows the SFP as unknown but the link comes up correctly.	When SFP for OC-12 is inserted.	None
CSCin98686	A redundant pair of RPM-XF cards fail after **show startup-config** on the primary RPM-XF when the auto_config_slot<slot_no> file is deleted.	Redundancy pair of RPM-XF cards.	None

Open Caveats in Release 12.3(11)T7

Table 3 lists caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00.

Table 3 Open Caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00

Caveat Number	Symptom	Conditions	Workaround
CSCei59221	Connections between AXSM-XG <-> RPM-XF do not pass traffic, after graceful hardware migration of redundant pair of AXSM-A/B/E cards to AXSM-XG.	Only those connections added between AXSM-A/B/E and RPM-XF before the AXSM-XG hardware upgrade process, do not pass traffic. New connections added between AXSM-XG and RPM-XF do not have this problem. Also the problem is seen only with the hardware upgrade of an AXSM-A/B/E redundant pair to AXSM-XG. Standalone card upgrades do not result in a connection problem.	Delete the connections which are in trouble and then re-add the connections between AXSM-XG and RPM-XF.
CSCei72576	The following error message and traceback were noticed in some RPM-XF cards and the destinations were unable to be pinged: %GENERAL-3-EREVENT:HWCEF: Failed to alloc Mtrie HW node Traceback = 4005B148 4005C398 4005C918 40066B5C 4028D634 4028DF6C 40294B84 4029AC5C 4063D470 40614C90	This problem occurs when many summary routes are advertised with continuous route updates and withdraws through BGP or IGP sessions. The PXF CEF memory for Level 4 gets exhausted, which results in the error message.	None.

Table 3 Open Caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCsb38738	RPM-XF reloads unexpectedly.	This problem occurs with RPM-XF running the 12.3(02) XZ image while copying Bulk file.	None.
CSCsb74429	Network delay or interruption can occur when there are RPM-XF GE cards in the network. Traceroute can occasionally take an extra hop through the RPM-XF GE card when it should not.	When there is at least one RPM-XF GE card and another IP device that does not actively speak in the same VLAN, traceroute sometimes shows the route to that device takes an extra hop through the RPM-XF GE card. Intermittent traffic storms may occur when there are 3 or more RPM-XF GE cards in the same VLAN.	Apply an inbound access-list to RPM-XF GE interface that prevents local VLAN forwarding. For example: ip access-list extended no-local-forwarding permit ip any host 192.168.1.100 permit ip any host 192.168.1.255 deny ip any 192.168.1.0 0.0.0.255 permit ip any any ! interface GigabitEthernet 1/0 ip address 192.168.1.100 255.255.255.0 ip access-group no-local-forwarding in This access-list stops traffic storms generated by RPM-XF, but does not fix the traceroute problem and may cause some operating systems to report that *ping* to a target device is denied. There are no effective workarounds for the traceroute or ping problems.

Open Caveats in Release 12.3(11)T6

Table 4 lists caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20.

Table 4 Open Caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20

Caveat Number	Symptom	Conditions	Workaround
CSCef05018	Disconnecting and reconnecting a Gigabit Ethernet cable on an RPM-XF may cause the TCP/IP connection to be lost on the VISM.	This symptom is observed on an RPM-XF that runs Cisco IOS Release 12.2(11)YP and Release 12.3T.	None
CSCeg23771	All compressed UDP packets from a RPM_PR CE are dropped by PE RPM_XF.	Configure basic frame-based MPLS and send UDP traffic from CE to PE. This condition was observed on an RPM-XF that runs Cisco IOS Release 12.3(11)T.	Unknown
CSCeh56264	The PXF resets abnormally in the network due to TBB Length Error.	Under normal conditions. No special trigger found. This condition was observed on an RPM-XF that runs Cisco IOS Release 12.3(2)XZ.	None. The microcode module reloaded abnormally which resulted in a short duration of outage as the hardware forwarding is disabled.

Open Caveats in Release 12.3(11)T3

Table 5 lists caveats in Cisco IOS Release 12.3(11)T3 for MGX Release 5.1.00.

Table 5 Open Caveats in Cisco IOS Release 12.3(11)T3 for MGX Release 5.1.00

Caveat Number	Symptom	Conditions	Workaround
CSCee75243	RPM-XF may reload abnormally during a rapid adding and removing of the service policy map.	While adding or removing service policy maps, the RPM-XF router reloaded abnormally with following error/traceback: %GENERAL-3-EREVENT: Policy map is in use. Traceback = 400BAD74 400BB498 400BB6A0	Unknown
CSCef05018	Disconnecting and reconnecting a Gigabit Ethernet cable on an RPM-XF may cause the TCP/IP connection to be lost on the VISM.	This symptom is observed on an RPM-XF that runs Cisco IOS Release 12.2(11)YP but could also occur in Release 12.3.	None
CSCeg23771	All compressed UDP packets from RPM_PR CE are dropped by PE RPM_XF.	Configure basic frame-based MPLS and send UDP traffic from CE to PE.	Unknown

Table 5 Open Caveats in Cisco IOS Release 12.3(11)T3 for MGX Release 5.1.00 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCeg24938	Continuously executes **clear ip mroute *** and causes RPM-XF to get reset.	While RPM-XF is configured as XF low speed, **clear ip mroute *** command was executed repeatedly which eventually caused the router to get reloaded abnormally.	Unknown
CSCeg27043	Peripheral Interface Manager (PIM) neighbors continue to flap after you have reloaded microcode.	This symptom is observed on a Cisco MGX 8850 series RPM-XF that runs Cisco IOS Release 12.3.	None
CSCeg40721	SAR tail drops seen on multicast PEs.	This problem was seen on a Cisco MGX8850 switch with RPM-XF cards running Cisco IOS Release 12.3(11)T images. Tail drops were observed on the SAR while sending bursty traffic to multiple multicast destinations.	Under investigation
CSCeg64074	The switch connection goes through the following states with the maximum PCR value: inSync, unknown, OnlyOnRPm	Create a switch connection between any two RPM_XF cards with service type VBR-nrt with a maximum PCR value.	None
CSCsa45189	Header compression is not working on an RPM-XF card that is configured for SAR-based CBWFQ.	This problem is seen when header compression is configured with a PPP configuration on a virtual template. This configuration is used because the PVC size is more than 768kbps and MLPPP does not support CoS for PVCs of this size.	Use a smaller PVC with MLPPP and cRTP.

Open Caveats in Release 12.3(7)T3

Table 6 lists caveats in Cisco IOS Release 12.3(7)T3 for MGX 5.0.10.

Table 6 Open Caveats in Cisco IOS Release 12.3(7)T3 for MGX Release 5.0.10

Caveat Number	Symptom	Conditions	Workaround
CSCea84387	A user session may pause indefinitely, causing a Cisco router to become unresponsive.	This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router through separate virtual type terminal (vty) sessions.	Allow only one user at a time to enter MQC commands.

Table 6 Open Caveats in Cisco IOS Release 12.3(7)T3 for MGX Release 5.0.10 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCec16481	A Cisco device running Cisco IOS and enabled for the 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 Cisco IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines, and all Cisco IOS images before 12.0 are not affected. Refer to the Security Advisory for a list of affected release trains.	Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml
CSCed05924	PXF reloaded abnormally due to software exception%PXF-2-FAULT:T0 SW Exception:CPU[t0r3c1] 0x00000180 at 0x0DE1 LR 0x084B.	MVPN traffic was being passed. No other activity was present on the card at that time.	Unknown
CSCed34575	An MPLS packet is transmitted without fragmentation even if the MPLS packet exceeds the outgoing interface MTU.	Occurs when the MPLS packet is greater than the outgoing interface MTU.	None
CSCed39641	SAR rx drops all packets because there is no buffer.	RPM-XF is configured as a PE in a frame-based or cell-based MPLS or VPN network. Executing the **sh pxf cpu buff leaked 0-5** or **clear interface sw1** command while the system is under load may cause a SAR rx failure.	None
CSCed48954	Traffic tail drops on the output of a Gigabit Ethernet interface even when the traffic rate is well below the interface limit.	Occurs after multiple Gigabit Ethernet interface flaps.	Reload the PXF using the **microcode reload pxf** command.
CSCed86771	Removing or inserting an RPM-XF while running call rate made the card reload/failed.	Occurs while running 360K Busy Hour Call Attempts (BHCA) with 120-second CHT. Upon removing an RPM-XF card and putting it back into the rack, this RPM-XF card rebooted and entered failed state.	None

Table 6 Open Caveats in Cisco IOS Release 12.3(7)T3 for MGX Release 5.0.10 (continued)

Caveat Number	Symptom	Conditions	Workaround
CSCee36771	A PPPoA interface constantly flaps when passing data with SAR-based CBWFQ enabled.	Observed under the following conditions: • SAR-based CBWFQ is enabled on a PPPoA interface. • The class default is assigned a small bandwidth (less than 10 percent). • All classes on the VC are congested.	Assign 10 percent bandwidth to the class-default of the policy map attached to the interface.
CSCee53246	The standby (secondary) RPM does not release the config_file boot variable after the primary redundant RPM card takes over after the **card switch over** command was executed.	This intermittent symptom was observed after a switchover from secondary RPM card to primary RPM card. The secondary (redundant) card is in standby state, but the **show bootvar** command still shows that the config_file variable is not null.	Unknown

Resolved Caveats

This section contains the list of resolved caveats in Cisco IOS Releases 12.4.x and 12.3.x.

Resolved Caveats in Cisco IOS Release 12.4(6)T1

Table 7 lists resolved caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00:

Table 7 Resolved Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00

Caveat Number	Description
CSCei13567	XFL: COSQ weight < MTU causes deficit counter wrap with bigger pkts
CSCei95224	Need high-watermark warning mechanism for PXF CEF memory usage (see hw-module pxf cef-mem-threshold, page 37)
CSCej23163	Error gige driver init if OIR-ed frontcard/backcard
CSCek24579	show inventory not supported on rpm-xf
CSCek27437	Snmp req to delete swconn from CWM should not delete PVC part
CSCek30114	Toaster client does not track PXF adjacency parts
CSCek32263	Need a routine to verify PXF iram parity after pxf crash
CSCsc20181	Need mechanism to disable TOD from PXM when RPM connected to NTP (see hw-module rpm pxm-tod-ignore, page 36)
CSCsc20181	Need mechanism to disable TOD from PXM when RPM connected to NTP
CSCsc56952	Humvee Serdes sync might not occur resulting in Data loss

Table 7 Resolved Caveats in Cisco IOS Release 12.4(6)T1 for MGX Release 5.3.00

Caveat Number	Description
CSCsc91990	ENT_API-4-NOPARENT message seen on insertion of GIGE backcards (Duplicates CSCek24579)
CSCsd05487	Limit vty lines to 250 for non-restricted mode export
CSCsd08392	RP-sourced control pkts are sent to the SAR class-default queue
CSCsd52064	Traffic policing is not working after removing and adding of diff policy
CSCsd55032	Multicast Outgoing Interface List not updated correctly in PXF
CSCsd76813	Police succeeds on only one interface when same policy is applied

Resolved Caveats in Release 12.3(11)T9

Table 8 lists resolved caveats in Cisco IOS Release 12.3(11)T9 for MGX Release 5.2.10

Table 8 Resolved Caveats in Cisco IOS Release 12.3(11)T9 for MGX Release 5.2.10

Caveat Number	Description
CSCeg32227	LSNT:Errors observed on Cards due to excessive tail drops
CSCei59221	Traffic doesnt pass after AXSM-XG graceful h/w migration
CSCei72576	Tracebacks and ping failure due to exhaustion of L4 pxf mtrie nodes
CSCej73880	ifOutUcastPkts and ifInUcastPkts decrements when queried 2 port gige
CSCsb01513	show rpm trapclient ctrblk has task state = 8
CSCsb34361	XFL:Cos queue size not updated properly when switching from WRED to EPD
CSCsb38738	RPM-XF reloads unexpectedly while copying bulk file due to exception
CSCsb47438	XFL:Cos Q creation fails while switching between WRED and EPD
CSCsb74429	RPMXF GE card should not process frame with MAC address to other devices
CSCsb93058	switchcdred on RPM-XF from Act to Stby shows interfaces admin down

Resolved Caveats in Release 12.3(11)T7

Table 9 lists resolved caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00.

Table 9 Resolved Caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00

Caveat Number	Description
CSCeh00486	Data structure error logged with Traceback
CSCeh34849	Packets out counter shows 0 in sh interface virtual-access stats CLI
CSCeh55603	PXF crashes observed on RPM-XF
CSCeh68799	SNMP: Entity MIB returns incorrect/null values
CSCeh92060	IOS ignoring CS packets sent by RPM-XF
CSCei00289	Need ability to see PXF XCM IPHC-data-structure addresses

Table 9 Resolved Caveats in Cisco IOS Release 12.3(11)T7 for MGX Release 5.2.00 (continued)

Caveat Number	Description
CSCei10711	If CS packets not responded to, RPM-XF punts all packets to RP
CSCei21134	SAR buffer oversubscription cannot be detected during qsize configs
CSCei37769	WRED thrsh recalc. can be undesirable in XFL with high XFH values
CSCei40059	CE1 to CE2 ping fails when CEF accounting is enabled on PE VRF interface
CSCin92488	Clear counters CLI does not clear match filters data rate counter
CSCsa97862	With TMS enabled, tracebacks seen on adding VRFs
CSCsb03279	Excessive recompiles of QoS policies
CSCsb25054	Remote PE crashes when telnet to remote CE is done from local PE or CE

Resolved Caveats in Release 12.3(11)T6

Table 10 lists resolved caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20.

Table 10 Resolved Caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20

Caveat Number	Description
CSCdz67845	The other counts field in the **show ip mroute** CLI command output is not accurate.
CSCed43120	Traffic rate distribution between classes during congestion is not according to the specified class bandwidth.
CSCee25068	RPM-XF card with SAR-based QOS failed with Data Path Check Failed logged.
CSCeg20467	**show pxf cpu cef verify** fails for 0.0.0.0/0 if the default route is not configured on the RPM-XF.
CSCeg23176	An RPM-XF is reset by the PXM because of an SCM poll timeout. A PCI information file is generated in the bootflash memory just before the RPM-XF resets.
CSCeg24938	An RPM-XF resets when you enter the **clear ip mroute *** command repeatedly.
CSCeg27043	PIM neighbors continue to flap after you have reloaded microcode.
CSCeg40721	Tail drops were seen on SAR CoS queues in XF low speed PEs.
CSCeg48606	A PXF stall error occurs, followed by a PXF crash.
CSCeg58427	It is difficult to detect any PXF programming errors in multicast FIB.
CSCeg61656	Bandwidth change on the bundle is not reflected on the RPM-XF switch sub i/f.
CSCeg64074	Switch connection creation with SCR at OC24 rate(1197656 kbps) fails.
CSCeg67839	The router stops responding when the CLI **sh pxf cpu cef** command is used in certain circumstances.
CSCeg69006	An alignment trace is seen in the RPM-XF log of the form %ALIGN-3-TRACE: Traceback = 4009E4C8 400AB6AC 404DB994 404DE5DC 404DEAA4 404DEE5C 404FDC4C 400AC160.

Table 10 Resolved Caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20 (continued)

Caveat Number	Description
CSCeg69019	When cwaChanDirectRoute is queried through SNMP, it returns a large int value instead of 1 or 2.
CSCeg80790	The commands **show policy-map int Switch1.x** and **show pxf cpu police** <*policymap-name*> can show different values for confirm burst (Bc) and there could be some drops on the policy map.
CSCeg84573	Traffic, including cell-based MPLS traffic, may be affected (that is, traffic may be dropped, or its behavior may be modified) after you have modified a QoS policy map that is already attached to an interface by way of adding a new class or deleting an existing class. Additionally, when a cell-based interface is affected by this symptom, traffic on other switch subinterfaces may also be affected even though the same policy map is not applied to these subinterfaces.
CSCeg89665	After you enter **switchredcd** on RPM-XF cards, the Gigabit Ethernet port on the RPM-XF back card does not forward or receive any traffic.
CSCeh05199	The **sh rpm iphc connection** command does not show all details for a flow on an IPHC-enabled interface.
CSCeh05517	It is difficult to detect PXF programming errors in multicast FIB's output interface list.
CSCeh05540	Packet statistics that are displayed under an L2 policy map are incorrect. The counters that show incorrect information are the Conformed packets/bytes and Exceeded packets/bytes counters.
CSCeh08537	The **sh rpm iphc hash-cids** command gives the hash-index but not the connection identifier (CID) for an IPHC flow.
CSCeh10391	An OamLpbkFail alarm is not cleared after a VISM card is reset.
CSCeh11228	Some data MDT may have the register flag stuck after card reload.
CSCeh12908	Unable to view the compressor side context on IPHC-enabled interfaces on an RPM-XF.
CSCeh13435	You cannot view the decompressor side context on IPHC enabled interfaces on an RPM-XF.
CSCeh14591	The following error message appeared %SYS-3-MEMLITE: Free lite called for non lite chunk by 0x400B93C4.
CSCeh15563	SAR CoSQ channel sometimes becomes stuck in close_pending state.
CSCeh15949	An extended access list does not function when it is applied to an interface even though the access list is configured correctly.
CSCeh22616	The output queue of a Fast Ethernet back card of a Cisco MGX RPM-XF may be stuck at 40/40.
CSCeh23404	The VC becomes inactive. ATM periodic process fails to delete the VC and reports tracebacks.
CSCeh27803	An MLP bundle is incompletely set up on an RPM-XF, and therefore the MLP traffic is lost.

Table 10 Resolved Caveats in Cisco IOS Release 12.3(11)T6 for MGX Release 5.1.20 (continued)

Caveat Number	Description
CSCeh30818	A traceback is generated when multicast traffic is flowing. This symptom is observed when a PIM is enabled on multiple interfaces and when the counters are cleared.
CSCeh35987	The policy map counter displays incorrectly after you modify a CoSQ channel parameter.
CSCeh44900	Tracebacks are seen while modifying the Access list.
CSCeh46004	A SAR ucode reload is not recorded.
CSCeh46547	Alignment errors logged with fast-switched IP packets sent over a Multilink interface.
CSCeh49205	Ping fails after enabling ip cef accounting.
CSCeh53494	Input policy map change causes the system to warn that the associated input service policy is being removed due to incompatible command usage.
CSCeh54816	L2 policing is incorrect. It shows a greater number of cells than used by the cRTP packet for certain packet sizes.
CSCeh61337	The commands **ip icmp rate-limit unreachable** and **ip icmp rate-limit unreachable DF** are always set at 500 ms.
CSCeh61775	It is difficult to detect any rewrite string errors in multicast FIB.
CSCeh67651	The policy map output counters are incorrect. They do not show the total number of packets, such as transmitted + dropped < input count. This problem manifests when there is congestion and is only seen for non-llq classes (excluding class-default).
CSCin90062	VSICMERR136 logged in an RPM-XF VSI slave for connections in CmtPend state.
CSCsa45270	The **show policy interface multilink** <*no:*> command shows discrepancy in total transmitted+ random drop + tail drop and the number shown to be received on the remote end.
CSCsa71055	Pings from a PE router to the Ethernet interface of a CE router fail.
CSCsa86250	The CPU use of a Cisco MGX series RPM-XF increases to 99 percent when a Gigabit Ethernet (GE) interface of a peer RPM-XF is shut down.

Resolved Caveats in Release 12.3(11)T3

Table 11 lists resolved caveats in Cisco IOS Release 12.3(11)T3 for MGX Release 5.1.00.

Table 11 Resolved Caveats in Cisco IOS Release 12.3(11)T3

Caveat Number	Description
CSCee63435	The RPM-XF VSI slave does not reply with extended VSI negative acknowledgement (NAK) error codes 51-54.
CSCee65241	In the **show policy-map interface** command, all police counters should be read as Layer 2 counters.
CSCef91218	An RPM-XF corrupts the DSCP values of traffic passing through.

Table 11 Resolved Caveats in Cisco IOS Release 12.3(11)T3 (continued)

Caveat Number	Description
CSCef36941	Apart from real time traffic streams, the RPM-XF card compresses the UDP traffic also on the Multilink interface configured for IP Header compression and connected to Customer router. The compressed UDP traffic received by the CE creates some problems thus making the CE unstable.
CSCef92881	Output of traceroute incorrectly shows the next hop entry for an interface on RPM-XF as 0.0.0.0 instead of showing the IP address of the interface.
CSCef95597	RPM-XF router reloads abnormally when the ATM encapsulation for a PVC is changed.
CSCeg10138	The 64-bit counters in the output of a **show policy-map** command may not provide correct information.
CSCeg16660	Load balancing of traffic works inconsistently if the traffic flow reaching the particular PE was already load balanced at a previous hop by another PE.
CSCeg16953	DBF tracebacks on RPM-XF by RPM-XF VSIS process.
CSCeg17058	There is not enough information to verify the exact cause of memory-related ECC errors for a PXF ASIC present on an RPM-XF.
CSCeg17274	When you enter a timeout value shorter than 8 seconds on an compression-enabled interface, the value is not configured. Instead, a timeout value of 8 seconds is configured.
CSCeg18940	Connection level parameter mismatch between RPM-XF and Cisco WAN Manager (CWM) Db.
CSCeg20768	The OSPF cost calculation is not triggered when the DBF update is received.
CSCeg24025	IPCP between MWR and RPM-XF does not come up after throttling Q2 on an MPSM.
CSCeg25053	There is no notification message in the log buffer or on the console related to the Switch Connection Synchronization applicable to Auto Resync or Manual Resync.
CSCeg27046	Important system and CPU register values are not stored into the Crashinfo file if the router reloaded abnormally.
CSCeg28876	no ip route-cache appears under the MLPPP interface in the configuration even though route-cache is enabled by default. In addition, no ip route-cache cef occasionally appears.
CSCeg31236	Spurious memory access is seen along with the traceback.
CSCeg34852	VCCI drops on RPM-XF after resetting the MPSM card.
CSCeg36182	The RPM-XF card does not come up after reload and some tracebacks are observed.
CSCeg47178	The **clear counters** command takes a long time to zero out the average offered/drop rate counters.
CSCeg65037	**swfpga cam** overwrites, which results in a dangling connection.
CSCeg65362	The **show policy interface** <*intf*> input command shows more packets are received than the **show interface** <*intf*> **precedence** command.
CSCin81995	The SAR engine on a RPM-XF shows buffer exhaustion, causing data drops.

Table 11 Resolved Caveats in Cisco IOS Release 12.3(11)T3 (continued)

Caveat Number	Description
CSCin84419	Multicast traffic is punted to the RP, the CPU utilization is high, and the output of the **show pxf cpu mroute vrf [vrf-name]** command shows that the "No_FS" flag is set for a (S,G) entry and does not clear.
CSCin84421	Traffic outage when switching from data MDT to a default MDT.
CSCin84494	CPU utilization is 99 percent.
CSCsa40567	The output of the **show rpm iphc cids [src-ip dest-ip src-udp-port dest-udp-port max-cids]** command does not show the CID values. Only zeros are seen in the command output.
CSCsa45197	When you enter the **show policy-map interface [interface-name] [output]** command for a switch subinterface, the drop rate counter always shows zero.
CSCsa81379	NetFlow Feature Acceleration has been deprecated and removed from the Cisco IOS. The global command **ip flow-cache feature-accelerate** is no longer recognized in any Cisco IOS configuration.

Resolved Caveats in Release 12.3(7)T3

Table 12 lists the resolved caveats in Cisco IOS Release 12.3(7)T3 for MGX 5.0.10 as of August 18, 2004.

Table 12 Resolved Caveats in Cisco IOS Release 12.3(7)T3 for MGX Release 5.0.10

Caveat Number	Description
CSCea85395	BGP suppressed prefixes are not reinstated after the condition is removed.
CSCed16744	Traffic does not resume after SAR is brought out of a hung state.
CSCed41381	Input drops on framed PVC i/f, causing the LDP session flap.
CSCed41823	Tx SAR stuck after micro rel sar tx/rx issued.
CSCed74882	CPUHOG Traceback on reload with large no of secondary IP addresses.
CSCed88043	The outgoing VCCI programmed in the FIB/TFIB in the PXF for a prefix is incorrect.
CSCed92418	Back to back clear int sw1 causes the VSI to go down on the PXM.
CSCee06261	RP crash on rpmxf_is_atm_mlp_configured while clear int sw1.
CSCee12415	Multicast traffic is not getting switched correctly.
CSCee23320	Router might reload upon deleting or reapplying a policy map.

Resolved Caveats in Release 12.3(2)T6

Table 13 lists resolved caveats in Cisco IOS Release 12.3(2)T6.

Table 13 Resolved Caveats in Cisco IOS Release 12.3(2)T6

Caveat Number	Description
CSCdy81782	No shut on the ppp interface before the VA stops responding causes the PXF to drop.
CSCeb05118	An RPM-XF that is configured as an eLSR may reload when deleting MPLS-type subinterfaces.
CSCec21461	On an RPM-XF, the input packet count for Virtual-Access interfaces are higher than the number of packets received.
CSCed22425	On an RPM-XF router, there is no way to know which eBGP path is chosen when there are multiple VRF interfaces to the VPN prefix.
CSCed41273	The PXF gets reloaded abnormally several times after the microcode reload.
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.
CSCed42706	On a Cisco RPM-XF router, the PXF does not increment the correct drop code when dropping packets.
CSCed46603	MIB walk on ifOutDiscards object OID returns an error message.
CSCed53155	After failure recovery, the SAR Segmenter is not programmed correctly.
CSCed62886	The 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.
CSCed71750	Virtual-Access counters do not match the ATM subinterface counters.
CSCed75086	When you issue the **show pxf cpu rewrite verification x.x.x.x** command, an error message appears, 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 (debug).
CSCed91750	S,G entries are not being created in the core.
CSCed68717	Incoming traffic is not being forwarded.
CSCed70687	PXF buffer allocate failure occurs on an eLSR.
CSCed78131	Checksum errors are reported on cRTP traffic streams.
CSCed83738	Packets on cRTP-enabled PPPoA interfaces that match classes other than class-default are 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.

Table 13 Resolved Caveats in Cisco IOS Release 12.3(2)T6 (continued)

Caveat Number	Description
CSCed94549	A compressed packet from an RPM-XF is rejected by the RPM-PR as a CRC error.
CSCed96053	Does not show precedence IP accounting for RTP/UDP compression packets.
CSCee00031	The average packet size displayed under show ip mroute count does not match the size of the multicast packet being sent.
CSCee00038	Protocols flap when the non-ATM (POS or Gigabit Ethernet) interfaces are congested by high traffic.
CSCee00685	Incorrect DSCP values are set on the IP packets.
CSCee02220	Multicast traffic flows use default MDT instead of data MDT for some VRFs.
CSCee02404	PXF buffer leak, loss of connectivity, BGP down on the PE-CE VRF link with cRTP enabled.
CSCee03726	PXF buffers are leaked.
CSCee07654	Starting on Multicast traffic on the CE occasionally puts the PXF on the PE in a loop. LDP/BGP/OSPF all go down and there is no data continuity.
CSCee11775	When PXF fails while a debugging operation is performed you may not be able to easily verify the string rewrite information of the PXF engine.
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, if the data path pings fail even though traffic is flowing through switch1, the data path feature recovery is enabled and this resets 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 fill up too 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 pxf cpu subblock** <*multilink interface*> command are displayed incorrectly.
CSCee30230	Traffic that matches a priority class may be dropped for a single prefix. However, traffic that matches other classes may pass correctly.
CSCee37181	On an RPM-XF, when there are multiple outgoing MPLS paths there could be inconsistency between the hardware and software MPLS forwarding table.
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.

Resolved Caveats in Release 12.3(2)T5

Table 14 lists resolved caveats in Cisco IOS Release 12.3(2)T5.

Table 14 Resolved Caveats in Cisco IOS Release 12.3(2)T5

Caveat Number	Description
CSCeb74859	BGP flap occurs when applying or removing an output policy map.
CSCec14218	Traceback messages.
CSCec84591	Barium Asserted CRC error when clear int sw1.
CSCec89536	Reassembler multi-bit error caused the card to crash.
CSCed00196	**show pxf tfib** does not display load balanced routes.
CSCed21634	Need to change exp bit on topmost label on egress interface.
CSCed30548	Input policy map does not match against mpls exp bit.
CSCed34585	Channel ID is incorrect for certain prefixes if multi-VC is enabled.
CSCed35834	Hub router with two POS up links crashed due to bus error.
CSCed35859	Must change the way PXF services the IP packets with option.
CSCed41293	Improve PXF CEF and TFIB command output.
CSCed41905	Automatic OIR occurred on RPM-XF card and the RPM-XF rebooted.
CSCed46492	Ethernet Port E2/1 on RPM-PR Card Gets Shutdown Upon Resetcd.
CSCed47631	SAR resetinfo files sometimes were not written to the bootflash.
CSCed48941	PE stops responding with no memory for XCM temp buffer logged.
CSCed49968	OSPF flaps between PE-LSC while congesting input hold queue.
CSCed50101	A 6-second wait is required before turning on ATM OAM to VXSM while RPM-XF GE is up.
CSCed54591	SAR crashinfo does not capture event log but resets the event log.
CSCed63090	Reload occurs when defragmenting ACL XCM memory.
CSCed69526	Process sleep not allowed while interrupts are disabled.
CSCed74712	SFP security check fails with 2-port Gigabit Ethernet card for new SFP.

Resolved Caveats in Release 12.3(2)T4

Table 15 lists resolved caveats in Cisco IOS Release 12.3(2)T4.

Table 15 Resolved Caveats in Cisco IOS Release 12.3(2)T4

Caveat Number	Description
CSCdx15989	Need debug information from **sh rpm mxt4400 chip** command.
CSCdx52061	Drop rate counter on output of **sh pol int**.
CSCdy32261	Traceback in config switch interface enters an incomplete command.
CSCea60559	lsr mib snmp agent consumes 99 percent CPU utilization forever.

Table 15 Resolved Caveats in Cisco IOS Release 12.3(2)T4 (continued)

Caveat Number	Description
CSCea74339	Data path VC (254/254) is not properly programmed.
CSCea76134	eiBGP load balancing does not work.
CSCeb05796	For a range of bandwidth, RPM-XF provides the lower end of range.
CSCeb10018	Tracebacks observed on reset card or when entering the **clear ip bgp** command.
CSCeb47748	Display VTMS info for to-RP link.
CSCeb59710	Protocols flap on eLSR when withdrawing LVCs.
CSCeb61055	Incorrect MPLS label built for VRF route.
CSCeb80653	Generate mxt4600_info file on fatal 4700 SAR errors and reset chip.
CSCeb84273	Interrupt statistics required in 2-port back card drivers.
CSCec09316	Packet with out-of-range CID should be dropped.
CSCec13765	Micro code reload clears the cRTP enable flag for ppoA links.
CSCec15993	In sar_mxt4400_info file, chip dump overwrites part of the data.
CSCec20821	PXF reload caused a card to stop responding with cell-based MPLS setup.
CSCec29812	CEF_scanner triggers high CPU use.
CSCec30428	Enhanced VTMS to handle possible hardware second timer update miss.
CSCec31168	mVPN Tunnel receive counters not implemented.
CSCec31864	RPM-XF sending wrong fields in Interface load info VSI-S message.
CSCec39423	TCB Leak (CSCea20818) and unicast fixes from CSCdx87287.
CSCec40662	RPM-XF reloads during **show pxf cpu rewrite tree** command.
CSCec42547	Incorrect MAC/Encap string in mpls forward table, traffic down.
CSCec43590	RPM-XF IPHC does not decompress 16-bit paks with IP options.
CSCec45704	Binding info not used by tfib/cef for some PEs prefix.
CSCec48318	TCB rel err reported incorrectly (CSCdw02481).
CSCec53230	Command to check consistency between ASIC forwarding & IOS TFIB.
CSCec53635	Channel_id is not updated sometimes after the main switch i/f resets.
CSCec60594	Link cannot be up when using 2-port POS with Y-cable redundancy.
CSCec60947	AVL memory leak suspected.
CSCec61293	RPM-XF reloads unexpectedly deleting MPLS switch subinterface.
CSCec62846	Failure on the data forwarding path was not detected.
CSCec63848	Some PXF drop counters are not cleared.
CSCec64570	Both local CEs cannot ping remote PE, and hop count is 13.
CSCec66381	SSI IPC errors during boot up.
CSCec67863	Memory leak when removing MDT.
CSCec76217	Check null ptr in VprEncIfcCfgGetMore (CSCea64395).
CSCec76702	Per packet load balance is not stable. Packets loss periodically.
CSCec77300	RPM-XF card reloaded.

Table 15 Resolved Caveats in Cisco IOS Release 12.3(2)T4 (continued)

Caveat Number	Description
CSCec87123	Carrier transition counter is not working.
CSCec78844	Check prev TCB is null before access (CSCdz38917).
CSCec85178	Reload due to L2 watchdog timer after **microcode reload** command.
CSCed00573	No HWIDB_SB_C10K_TT (clear arp caused tracebacks).
CSCed07063	Certain sequence of ftctrace/ttctrace causes Cisco IOS crash.
CSCed07231	rpmxf ucode error would cause protocol flags if PQ congested.
CSCed07254	rpmxf ucode error would cause PXM stall error.
CSCed07480	Cisco IOS shows SFP MISSING for Hitachi Cable SFP.
CSCed07712	SARCMDTIMEOUT: SAR command timeout, device Reassembly SAR.
CSCed11101	Traffic cant recover after POS OIR when vrf configured on POS.
CSCed15811	On data SAR fatal interrupts, SAR CMD TIMEOUTs are seen.
CSCed17550	Clearing PXF stat and drop counters cause mem leak.
CSCed20528	Periodic function keeps on invoking restart PVC after clear int sw1.
CSCed22568	Under low memory condition system might get reset due to missing call to reset_interrupt_level() routine.
CSCed22895	Possible array out of boundary.
CSCed23060	Incorrect column number passed during a PXF write.
CSCed23216	eiBGP multipath load balancing failed for some IP addresses.
CSCed23982	PXF stops responding due to DMA stall error.
CSCed28404	PXF buffer leak occurs for tag switched packets with input policymap.
CSCed28880	ATM OAM not tracking the Gigabit Ethernet link status on an RPM-XF.
CSCed31769	Multicast and output logging conflict (port CSCec60999).
CSCed33563	Memory leak (ec66881) and VSI Core Code Audit fixes.
CSCed35983	Cannot CC to the RPM-XF from the PXM.
CSCed37755	All VCs were deconfigured in SAR after a microcode reload.

Resolved Caveats in Release 12.3(2)T2

Table 16 lists resolved caveats in Cisco IOS Release 12.3(2)T2.

Table 16 Resolved Caveats in Cisco IOS Release 12.3(2)T2

Caveat Number	Description
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.
CSCdw86381	**cnfpnportcac** command causes traceback if bandwidth used is greater than the minimum bandwidth requirement.

Table 16 Resolved Caveats in Cisco IOS Release 12.3(2)T2 (continued)

Caveat Number	Description
CSCdx06018	Multiple VBR flows hash to same PXF queue caused tail drops.
CSCdx92871	iBGP load balancing did not work when two CEs are in different VPNs.
CSCdy05346	Missing param-groups in the Switch Get Configuration Response from a VSI slave message.
CSCdy17457	**sh int** shows incorrect packet number after initiating a **shut** or **no shut** command on the interface.
CSCdy26882	Interface counters show incorrect values after back card OIR.
CSCdy42274	The PXF does not recover after a reload at high traffic rates.
CSCdy73751	Certain hardware error interrupts caused the Tx Gigabit Ethernet traffic to stop.
CSCdz23621	Standby RPM-XF VSI master endpoint ID is not cleared on PXM.
CSCdz86609	Packet drop observed at switch interface1 when traffic was flowing through.
CSCea15938	GTS shapes too aggressively for POS or Gigabit Ethernet interfaces.
CSCea27838	SYS-3-CPUHOG traceback logged and card hung for awhile.
CSCea60343	Connection goes into mismatch.
CSCeb05118	RPM-XF stopped responding when you delete the sw1.1 mpls interface.

Compatibility Notes

This section contains compatibility information for the RPM-XF card.

RPM-XF Boot File and Firmware File Names and Sizes

Table 17 displays the RPM-XF boot and firmware file names and sizes for this release.

Table 17 RPM Boot and Firmware File Names and Sizes

	File Name	File Size—bytes
Boot File	rpmxf-boot-mz.124-6.T1	4260824
Firmware File	rpmxf-p12-mz.124-6.T1	11151308
Firmware File (Crypto)	rpmxf-k9p12-mz.124-6.T1	11928296

RPM-XF Compatibility Matrix

Table 18 displays the RPM-XF compatible software versions for this release.

Table 18 RPM -XF Compatible Software Versions

MGX S/W Release	Cisco IOS Release	CWM
5.3.00	12.4(6)T1 12.3(11)T8 12.3(11)T6	15.3.00
5.2.10	12.3(11)T9	15.1.50
5.2.00	12.3(11)T7	15.1.50
5.1.20	12.3(11)T6	15.1.00
5.1.00	12.3(11)T3	15.1.00
5.0.10	12.3(7)T3	15.0.00 P2
5.0.00	12.3(2)T5	15.0.00
5.0.00	12.3(2)T6	15.0.00
4.0.15	12.3(2)T4	12.0.00.2
4.0.12	12.3(2)T2	12.0.00.2
4.0.10	12.2(15)T5	12.0.00.1

MGX RPM-XF Hardware

Table 19 shows front card and back card compatibility for the RPM-XF hardware supported in this release. The table lists the card name, part numbers, the minimum version and the minimum revisions of each card supported. The minimum version is identified by the last 2 digits of the 800-level numbers.

Table 19 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 20 shows the SFP compatibility matrix for the Cisco MGX Gigabit Ethernet and POS back cards.

Table 20 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

For Cisco IOS firmware, go to Cisco.com at:

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.

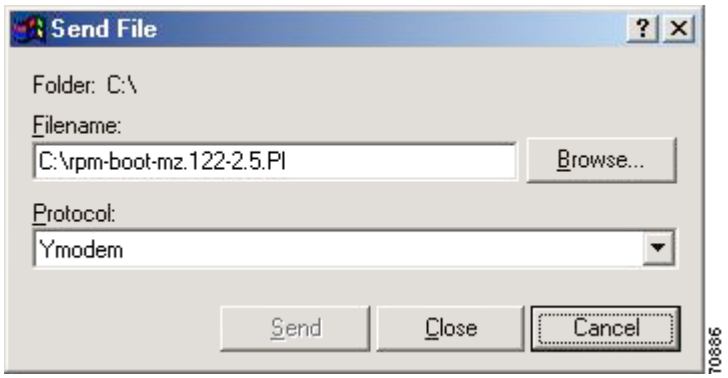
Note If you do not find the xmodem commands, then the xmodem feature is not available on this rommom version. In that case, you must return the card to Cisco.

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 To start the image transfer, use the **Transfer > Send File** option in HyperTerminal.



In the Filename box, browse and choose the image file to be downloaded. Because 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 window appears and transfer starts. (The transfer may not start immediately; wait for some time and it should start.)

The system resets and boots with a new software image.

Resolved Caveats in Cisco IOS Release 12.2.x Baseline

This section contains lists of the resolved caveats in the 12.2.x baseline.

Resolved Caveats in Release 12.2(15)T5

Table 21 lists resolved caveats in Cisco IOS Release 12.2(15)T5.

Table 21 Resolved Caveats in Cisco IOS Release 12.2(15)T5

Caveat Number	Description
CSCeb06375	An access list may fail to work as configured.
CSCea49948	Multiple crashinfo files may be saved on a 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.
CSCea93735	Control traffic may not be dequeued from a PXF processor towards an RPM-PR.

Resolved Caveats in Release 12.2.15T

Table 22 lists resolved caveats in Cisco IOS Release 12.2.15T.

Table 22 Resolved Caveats in Cisco IOS Release 12.2.15T

Caveat Number	Description
CSCea49948	Multiple Crashinfo due to IPC Messages. Multiple crashinfo files are generated, filling the bootflash of RPM-XF card.
CSCdz82543	Cannot cc to RPM-XF due to Messages on the Console. You may not be able to log into a 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 appear.
CSCdx08155	On LSC, querying of LVC statistics for an XtagATM interface would not abort command upon user entering a **Control-C**. If the user uses the **show xtagatm cross-connect traffic** to query on LVC statistics, normally, the user can quit the command in the middle by giving the Control-C sequence. However, the CLI does not return the prompt until the VSI master logic complete requesting statistics for all LVCs.
CSCdy26703	A ping from a CE to a PE may fail, and Parallel Express Forwarding (PXF) may stall.
CSCdy27120	Traffic does not flow through a VLAN on Gigabit Ethernet interface.
CSCdy65600	The output and input flow control parameters of a Gigabit Ethernet interface are displayed as ? “aused”.
CSCdz70762	Multi-vc traffic traveling on a particular precedence goes out to a queue with an incorrect precedence.
CSCdz82543	You may not be able to log into an RPM-XF, although when you display the status of the module from a PXM45 controller, no irregularities are shown. If you manage to establish a console connection into the RPM-XF, continuous traceback messages may appear.

Table 22 Resolved Caveats in Cisco IOS Release 12.2.15T (continued)

Caveat Number	Description
CSCea05477	After policy map is created, RPM-XF resets.
CSCin32860	Access list info of snmp-server community lost after RPM-XF reset.

Resolved Caveats Prior to Release 12.2.15T

Table 23 lists resolved caveats prior to Cisco IOS Release 12.2.15T.

Table 23 Resolved Caveats prior to Cisco IOS Release 12.2.15T and Earlier

Caveat Number	Description
CSCdw20568	Cisco Class-Based QoS mib (CISCO-CLASS-BASED-QOS MIB) is not supported on RPM-PR and RPM-XF cards.
CSCdw55382	The output of the command **sh swi conn vcc/vpc** does not correctly show the value of the maximum cost field.
CSCdw57105	Show sub-interface counter shows incorrect value.
CSCdw68738	Cobalt From RP Own Errors counter increments in **show hard pxf dma count** output. This does not affect data/traffic.

CSCdw69661	Invalid Epid Error message observed:
	`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`

CSCdw88019	Loopbacks provided on Gigabit Ethernet back card should be renamed to internal and “external from mac and driver, respectively.
CSCdw88767	Humvee counters show improper value and counters cannot be cleared.
CSCdw95563	After increasing the PCR value of PVP, traffic was dropped at a new rate.
CSCdx00982	SNMP **get** returns a different value for PCR/SCR from the configuration.
CSCdx12730	All the PVCs on the switch1 interface entered inactive state.
CSCdx16897	Performance issue observed in cleaning up and creating LVCs.

CSCdx44836	Modifying an existing PVP caused the following VSI error to appear 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`

CSCdx46583	Must verify Cisco IOS images on PXM hard drive and in RPM-XF flash.
CSCdx49122	**dspcd** <*slot#*> for RPM-XF slot does not show the full CLEI code/Serial number. One character at the end is missing.
CSCdx52025	Could not correlate output packets dropped on sub-interface with switch1 interface packet drop counters.
CSCdx55586	Setting ccCopyEntryRowStatus to ACTIVE returned general error status even if the row is correctly configured.

Table 23 Resolved Caveats prior to Cisco IOS Release 12.2.15T and Earlier (continued)

Caveat Number	Description
CSCdx58504	RPM-XF **show switch conn vcc|vpc** displays a network service access point (NSAP) in the following format: `47.0091.8100.0000.0001.6443.6c58.0000.0109.1802.00` This is not consistent with the PXM **dspcons** display.
CSCdx62385	Flapping of BGP caused an RPM-XF reload.
CSCdx64337	After changing the console baud rate the console behaved unpredictably.
CSCdx64361	ROMmon console froze up after pasting a large buffer.
CSCdx69702	The output counters displayed under **show policy-map int** <*sw1.x*> were not incremented.
CSCdx71190	A software-forced reload occurred on a router and the OSPF process failed.
CSCdx76951	There was humvee error on RPM-XF card.
CSCdx80500	A CLI command was needed to show the history of the messages that an RPM-XF received from the Shelf Manager on a PXM.
CSCdx87265	Deletion trap is not sent out for notOnRpm connections.
CSCdx91454	The status LEDs for the management back card are not illuminated correctly.
CSCdx93773	Packet drop on egress subinterface is below the configured rate.
CSCdy02182	When the Gigabit Ethernet device driver detects an error with the link to the front card, it does not automatically try to correct the situation properly.
CSCdy03275	Traffic is not passing in frame-based MPLS network when an RPM-XF is configured as a P router.
CSCdy05871	Tail drops on PXF queue while sending traffic at OC-12 rate.
CSCdy09544	Low Latency Queue (LLQ) starves low priority traffic.
CSCdy11581	Received traps for Fast Ethernet Interface Down(60662) and Fast Ethernet Interface up(60661) had incorrect *ifName* contents.
CSCdy15295	cbQosQueueingStats and cbQosREDClassStats MIB entries are not populated.
CSCdy23757	Data stopped flowing from VLAN after removing and inserting Gigabit Ethernet back cards.
CSCdy26495	class-map output queue packet counter does not show the correct number of packets.
CSCdy26755	Execution of PXM command **dspcd** for the RPM-XF card did not show 800 Level Rev number for the front card and the back card.
CSCdy27852	Excessive delay for LLQ packets.
CSCdy28132	Traffic forwarding stops. Traffic was forwarded to incorrect VC.
CSCdy30260	Protocol flap was observed and data labeled transfer stopped temporarily on an RPM-XF when an RPM-XF card when an adjacent slot was removed.
CSCdy31406	RPM-XF frame-based P router's PXF reloaded after shut PE subinterface.
CSCdy37576	Cannot add a dax connection between the RPM-XF (10) and the AXSM (1).
CSCdy38362	Line Alarm seen on Gigabit Ethernet interface on MGX-1GE even when administratively down.

Table 23 Resolved Caveats prior to Cisco IOS Release 12.2.15T and Earlier (continued)

Caveat Number	Description
CSCdy39423	Traffic stopped on Gigabit Ethernet interface when enabling autonegotiation parameter.
CSCdy39806	No switch partition configured traceback error logged.
CSCdy39861	Spurious memory traceback error logged when disable VRF forwarding under switch subinterface.
CSCdy40930	LLQ packets dropped on SAR because of lack of buffers.
CSCdy41773	In case of Gigabit Ethernet back card initialization failure, configuring it further may cause the RPM-XF card to reboot.
CSCdy45515	Connection endpoint on an RPM-XF did not generate RDI upon receiving AIS.
CSCdy51893	Class queues do not get programmed correctly. Class-based weighted fair queuing (CBWFQ) may not work correctly.
CSCdy53728	LLQ when defined with class queues does not achieve full SCR and improperly distributes traffic between the queues.
CSCdy55202	**sh pol int** shows zero bandwidth for all the classes.
CSCdy56345	After removing and inserting a POS back card, “Assertion Failure” tracebacks were observed.
CSCdy71426	All of the traffic on the PXF stopped.
CSCdy75485	All Layer 2 management packets dropped, which caused all interfaces that depend upon keepalives to transition to the down state.

Related Documentation

The *Cisco RPM-XF Installation and Configuration Guide, Release 5.2* is located at:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/rel52/rpm/rpmxf/icg/index.htm

Product documentation for the Cisco MGX 8850 Release 5.2 is located at:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/rel52/index.htm

Cisco IOS documentation for Cisco IOS Release 12.4(6)T1 is located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/index.htm

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/en/US/support/index.html

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 engineer. The TAC Service Request Tool is located at :

- TAC Service Request Tool - Login Required
  http://tools.cisco.com/ServiceRequestTool/create/launch.do

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 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

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

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