Multi-Service IronWare Software R02.7.03a for Brocade BigIron RX Series Switches

Release Notes v1.0

January 14, 2011

Document History

Document Title	Summary of Changes	Publication Date
Multi-Service IronWare Software R02.7.03 for Brocade BigIron RX Series Switches Release Notes v1.0	Release 02.7.03a	January 2011

Contents

Supported devices for Multi-Service IronWare R02.7.03a

This software release applies to the following Brocade products:

- BigIron RX-4 Switch
- BigIron RX-8 Switch
- BigIron RX-16 Switch
- BigIron RX-32 Switch

Note: The software release described in these release notes can only be used on the devices specified above.

All information required to operate the BigIron RX Series Switch is described in the *BigIron RX Series Configuration Guide* or the *Brocade BigIron RX Series Installation Guide.*

Enhancements

R02.7.03a

There are no enhancements in R02.7.03a.

R02.7.03

Enhancement	Descriptions	Described in…
Support for active cable for 16-port 10 Gigabit Ethernet module	10 Gbps Direct Attached Small Form-Factor Pluggable (SFP+) copper cable (1m, 3m, 5m) is available for the 16-port 10 Gigabit Ethernet module	Book: Brocade BigIron RX Series Installation Guide
Monitoring I2C failure on a management module	The **show logging** command can be use to monitor I2C failures.	Book: *Brocade BigIron RX Series Installation Guide*
Rebranded show version command output	The output of the **show version** command now shows "Brocade Communications"	Book: *Brocade BigIron RX Series Installation Guide*
Rebranded RADIUS	Vendor specific attributes for RADIUS have been renamed to "brocade-command-string", "brocade-privilege-level", and "brocade-command-exception-flag"	**Book**: *BigIron RX Configuration Giuide* **Chapter**: Securing Access to Management Functions **Section**: Configuring RADIUS security
MAC Port Security	The MAC Port Security feature has been updated for the 02.7.03 release.	**Book**: *BigIron RX Configuration Giuide* **Chapter**: Using the MAC Port Security Feature and Transparent Port Flooding

Enhancement	Descriptions	Described in…
Syslog update	The System Log has been updated as follows: • Separate buffers for static and dynamic logs • Entries in the static log buffer are cleared at reset or reload, while entries in the dynamic log are preserved • Log buffer size cannot be changed. The log buffer size is set at 3800 lines • A **show logging** command is now available at the monitor level for Active and Standby Management Processors	**Book**: *BigIron RX Configuration Giuide* **Chapter**: Using Syslog

Feature support

Below is a list of all the features supported on the BigIron RX switches. See Unsupported features, for features not supported.

Supported features

Category	Feature description
System level Features	
• Cisco Discovery Protocol (CDP)	Allows you to configure a Brocade device to intercept and display the contents of CDP packets. This feature is useful for learning device and interface information for Cisco devices in the network.
• CLI Logging	
• Denial of Service (DoS) protection	Protection from SYN attacks Protection from Smurf attacks
• Foundry Discovery Protocol (FDP)	Enables Foundry devices to advertise themselves to other Foundry devices on the network.
• High Availability	OS Layer 2 Hitless Software Upgrade

Category	Feature description
• Management Options	Serial and Telnet access to industry-standard Command Line Interface (CLI) SSHv2 TFTP Web-based GUI SNMP versions 1, 2, and 3 IronView Network Manager
• Security	AAA Authentication Local passwords RADIUS Secure Shell (SSH) version 2 Secure Copy (SCP) TACACS/TACACS+ User accounts 802.1x: All EAP types, including MD5, TLS, TTLS, and PEAP Multi-device port authentication **Note:** Telnet, SSH, Web and SNMP servers are disabled by default, and can be enabled selectively.
• CPU protection:	There are no CLI commands for CPU protection. The BigIron RX forwards unknown unicast, broadcast and multicast packets in hardware; therefore, the CPU is automatically 'protected' from having to handle too many packets.
• Logging	Multiple SysLogD server logging
• sFlow	sFLow version 5
• Uni-directional Link Detection (UDLD)	Monitors a link between two devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices.

Layer 2 features

• 802.1d	Spanning Tree Protocol (STP) and Single Spanning Tree Protocol (SSTP)
• 802.1p	Quality of Service (QoS) queue mapping

Category	Feature description
• 802.1q	see VLANs, below
• 802.1s	Multiple Spanning Tree Protocol (MSTP)
• 802.1w	Rapid Spanning Tree Protocol (RSTP)
• 802.1x	Port Security
• 802.3ad	Dynamic Link Aggregation on tagged and untagged trunks
• Jumbo packets	Layer 2 jumbo packet support
• Layer 2 Hitless failover	
• Layer 2 IGMP Snooping	
• MAC Filtering	MAC filtering and address-lock filters to enhance network security
• Foundry MRP	Metro Ring Protocol (MRP) Phase 1 and Phase 2
• PVST / PVST+	Per-VLAN Spanning Tree (PVST)
• Rate Limiting	Port-based, port-and priority-based, port-and vlan-based, and port-and-ACL-based rate limiting on inbound ports are supported.
• SuperSpan	A Brocade STP enhancement that allows Service Providers (SPs) to use STP in both SP networks and customer networks.
• Topology Groups	A named set of VLANs that share a Layer 2 topology. You can use topology groups with the following Layer 2 protocols: STP Foundry MRP VSRP 802.1w
• Trunk Groups and LAG	Allows you to manually configure multiple high-speed load-sharing links between two devices or between a device and a server.

Category	Feature description
• VLANs	802.1Q tagging Port-based VLANs Super Aggregated VLANs (SAV) Dual-mode VLAN ports Transparent Port Flooding VLAN ID to MSTP Instance Pre-assignment Private VLANs
• VSRP	Layer 2 Virtual Switch Redundancy Protocol (VSRP) Layer 3 Virtual Switch Redundancy Protocol (VSRP) VSRP and MRP Signaling
• Layer 2 ACLs	Replaces MAC filters
• Layer 2 PIM Snooping	

Layer 3 features

• ACLs	Standard, Extended, and Super Inbound ACL logging ACL editing
• BGP	BGP routes BGP peers BGP dampening Graceful Restart
• FDR	Foundry Direct Routing
• IP Forwarding	IPv4 Routing IPv6 Routing

Category	Feature description
• IP Static entries	Routes ARPs Virtual interfaces Secondary addresses
• IS-IS	Routes BGP peers BGP dampening
• Multicast Routing	Multicast cache L2 IGMP table DVMRP routes PIM-DM PIM-SM PIM-SSM IGMP v1, v2, v3 snooping PIM-SM snooping (IPv4 only)
• OSPF	OSPF routes OSPF adjacencies – Dynamic OFPF LSAs OSPF filtering of advertised routes
• PBR	Policy Based Routing (Release 02.2.01 and later)
• RIP versions 1 and 2	RIP routes
• VRRP and VRRPE	Virtual Router Redundancy Protocol (VRRP) and VRRP Extended (VRRPE)

IPv6 features

• IPv6 ACLs	Extended ACLs
• IPv6 Routing Protocols	RIPng OSPFv3 BGP4+

Unsupported features

The following features are not supported in software release 02.7.02 on BigIron RX:

- AppleTalk
- Dynamic IP Routing
- IPX
- Mirroring across VLANs
- MPLS
- NAT
- RARP
- VLANs
    - VLAN translation
    - Subnet VLANs
- Source IP Port Security

Software image files for Multi-Service IronWare R02.7.03

The following Software Image Files are available for Multi-Service IronWare R02.7.03 for the BigIron RX Series Switches.

Software image files

Module	Image type	Image name
Unified Image	N/A	rx02703a.bin
Management Module	Boot and Monitor	rmb02703a.bin
	IronWare	rmpr02703a.bin
BigIron RX-4, BigIron RX-8, and BigIron RX-16	FPGA	mbridge
BigIron RX-32		mbridge32
Interface Module	Boot and Monitor	rlb02703a.bin

Module	Image type	Image name
	IronWare	rlp02703a.bin

Images and procedures required

The software images required and the procedures for upgrading have been changed as described in the following sections:

- Upgrading Software Images as Required by Version – This sub-section describes the procedures required for your software upgrade depending upon the version you are upgrading from or to. Links are provided to the required procedures as required.

- Displaying the Version Information – This sub-section describes the commands that allow you to determine the contents of the BigIron RX Series switch's flash memory and how to read the output of those commands.

- Upgrading the device's Monitor and Multi-Service IronWare Image – This sub-section describes the procedures required for upgrading the BigIron RX Switches Monitor and Multi-Service IronWare software image.

- Upgrading the device's Boot Images – This sub-section describes the procedures required for upgrading the BigIron RX Series Switches Boot software images. [Upgrade required only if mentioned in Release Notes]

- Rebooting the device – This sub-section describes the procedures required for rebooting the device after upgrading the software images.

Upgrading the Multi-Service IronWare software

When performing this upgrade, you will usually only need to upgrade Unified Multi-Service IronWare image. The boot image will only need to be upgraded as specifically directed in the relevant release notes.

The steps for this upgrade include the following:

1. Determine the versions of the software images currently installed and running on the switch.

2. Upgrade the Device's Unified Multi-Service IronWare Image.

3. Reboot the BigIron RX Series switch.

4. In most cases, this is all that will be required. If you are directed by the release notes to upgrade the Boot image, use the upgrade the BigIron RX Series switches boot image procedure presented later in this document.

5. Reboot the BigIron RX Series Switch.

Displaying version information

Prior to upgrading the images on a BigIron RX Series switch, it is advisable to check the versions already installed. It is also useful to check the versions installed immediately after an upgrade has been done to

make sure that you have installed the versions required in your installation. The following sections describe how to use the **show version** commands to display this information.

You can display version information for a BigIron RX using the **show version** command as shown in the following:

```
BigIron RX Router#show version
===========================================================================
HW: BigIron RX Router
BigIron RX-16 CHASSIS (Serial #: Not Exist,  Part #: Not Exist)
RX-BI-SFM3 Switch Fabric Module 1 (Serial #: PR23050164,  Part #: 31523-100A)
FE 1: Type fe200,  Version 2
FE 2: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
RX-BI-SFM3 Switch Fabric Module 2 (Serial #: SA11061693,  Part #: 31523-200B)
FE 1: Type fe200,  Version 2
FE 2: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
RX-BI-SFM3 Switch Fabric Module 3 (Serial #: SA04071303,  Part #: 35523-200C)
FE 1: Type fe200,  Version 2
FE 2: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
RX-BI-SFM3 Switch Fabric Module 4 (Serial #: PR23050160,  Part #: 31523-100A)
FE 1: Type fe200,  Version 2
FE 2: Type fe200,  Version 2
FE 3: Type fe200,  Version 2
===========================================================================
SL M2: RX-BI-MR2 Management Module (High Value) Active (Serial #: PR23050106, Part #: 31524-
000A):
Boot     : Version 2.7.3T145 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:24:18 labeled as rmb02703
  (439582 bytes) from boot flash
Monitor  : Version 2.7.3T145 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:24:18 labeled as rmb02703
  (439582 bytes) from code flash
IronWare : Version 2.7.3T143 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:39:36 labeled as rmpr02703
  (4538957 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 21
916 MHz Power PC processor  (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
2048 MB DRAM
Active Management uptime is 13 minutes 14 seconds
===========================================================================
SL M1: RX-BI-MR2 Management Module (High Value) Standby (Serial #: PR23050077, Part #: 31524-
000A):
Boot     : Version 2.7.3T145 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:24:18 labeled as rmb02703
  (439582 bytes) from boot flash
Monitor  : Version 2.7.3T145 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:24:18 labeled as rmb02703
  (439582 bytes) from code flash
```

```
IronWare : Version 2.7.3T143 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:39:36 labeled as rmpr02703
 (4538957 bytes) from Primary
Board ID : 00 MBRIDGE Revision : 21
916 MHz Power PC processor  (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
2048 MB DRAM
Standby Management uptime is 12 minutes 0 seconds
========================================================================
SL 1: RX-BI-24C 24-port 1 GbE Copper Module (Serial #: SA32090569, Part #: 35521-003D)
Boot     : Version 2.7.3T155 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:23:18 labeled as rlb02703
 (307473 bytes) from boot flash
Monitor  : Version 2.7.3T155 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:23:18 labeled as rlb02703
 (307473 bytes) from code flash
IronWare : Version 2.7.3T157 Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
Compiled on Aug 27 2010 at 01:51:10 labeled as rlp02703
 (2334914 bytes) from Primary
FAP 1 version: 3
FAP 2 version: 3
FAP 3 version: 0
FAP 4 version: 0
660 MHz Power PC processor 440GP (version 8020/0020) 330 MHz bus
512 KB Boot Flash (AM29LV040B), 16 MB Code Flash (MT28F640J3)
512 MB DRAM, 8 KB SRAM, 0 Bytes BRAM
LP Slot 1 uptime is 11 minutes 57 seconds
.
.
.
All show version done
```

The fields are described in the Code Flash and Boot Flash Information, which appears above.

Different image information

Management Modules

This field	Displays
Boot Image	Indicates the boot image running in the management module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Compilation date and time – The date and time that Brocade compiled the image.
Monitor Image	Indicates the Monitor image running in the management module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Compilation date and time – The date and time that Brocade compiled the image.
IronWare Image	Indicates the IronWare image running in the management module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image, of the image change, and the check sum changes. • Compilation date and time – The date and time that Brocade compiled the image.

Interface Modules

This field	Displays
Boot Image	Indicates the boot image running in the interface module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Compilation date and time – The date and time that Brocade compiled the image
Monitor Image	Indicates the Monitor image running in the interface module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image. • Compilation date and time – The date and time that Brocade compiled the image.
IronWare Image	Indicates the IronWare image running in the interface module. The output displays the following information about the image: • Version – "2.2.1Txxy" indicates the image version number. The "Txxy" is used by Brocade for record keeping. The "xx" indicates the hardware type, while the "y" indicates the image type. • Size – The size, in bytes, of the image, of the image change, and the check sum changes. • Compilation date and time – The date and time that Brocade compiled the image.
FPGA Version Information	The following Images are only displayed from the **show version** command: • MBRIDGE Revision – The version number of the MBRIDGE FPGA installed on the Management module for the BigIron RX-16/8/4 • MBRIDGE32 Revision – The version number of the MBRIDGE32 FPGA installed on the Management module for the BigIron RX-32. • SBRIDGE Revision – The version number of the SBRIDGE FPGA installed on the BigIron RX-32 Switch Fabric modules.

Backing up the current software images

Before performing a software upgrade, Brocade recommends backing up the following current software images in the device's flash memory.

Syntax: cp <original-file-name> <backup-file-name>

Unified software image upgrade

You can use the Unified Software Image Upgrade procedure to upgrade the Monitor and the Multiservice Ironware image of both the management module and also the interface modules. You can use the command shown below to upgrade the Images. You can set parameters to limit images being copied and to direct images to be copied to the secondary image location to a later release.

1. Copy the unified software image (rx02703a.bin) from a TFTP server to the switch.

   For example, to copy the entire unified software image from a TFTP server at IP address 10.10.12.12, use the following command.

   ```
   BigIron RX# copy tftp image 10.10.12.12 rx02703a.bin
   ```

2. Reboot the management module using the reload command.

3. If you are using SSH v2, you must clear the crypto key using the crypto key zeroize command after you upgrade. Then, regenerate a new crypto key using the crypto key generate command.

This is the most common upgrade method. After reload all the cards in the system will be running the new monitor and Multiservice Ironware image.

You can also upgrade the boot images of the Management module and the interface module using the unified software image upgrade command along with the Monitor and System Image. This should be done only if it's mentioned in the release notes that the upgrade of the boot Images are necessary. We can use the following option with the above mentioned command to upgrade boot image along with monitor and system image as shown below.

```
BigIron RX# copy tftp image 10.10.12.12 rx02703a.bin lp-boot mp-boot
```

Syntax: copy tftp image <TFTP-server-ip-addr> <image-name> [lp-boot | lp-sec | mp-boot | mp-sec | mbridge]

The <TFTP-server-ip-addr> variable is the IP address for the TFTP server you are downloading the image from.

The <image-name> variable is the name of the unified software image you want to download to the switch.

The **lp-boot** parameter specifies that you want to download the new interface module boot image.

The **lp-sec** parameter specifies that interface image be copied to the secondary location in flash.

The **mbridge** parameter tells the BigIron RX to copy the MBRIDGE image. It will now include two MBRIDGES; one for BigIron RX-16/8/4 (mbridge.xsvf) and one for the BigIron RX-32(mbridge32.xsvf).

The **mp-boot** parameter specifies that you want to download the new management module boot image.

The **mp-sec** parameter specifies that management image be copied to the secondary location in flash

Upgrading the images Independently

Note: Using the unified approach is the easier single step process and also the preferred one.

If you don't want to use the unified software upgrade procedure to upgrade your modules boot, monitor and system images, you can do them one by one separately, as described in the sections below.

Upgrading the management module Monitor boot images

To upgrade the management module monitor and boot image, perform the following steps:

1. Place the new boot images on a TFTP server to which the BigIron RX system has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new monitor and boot images to the BigIron RX. Enter one of the following commands at the Privileged EXEC level of the CLI (example: `BigIron RX#`):

**Command syntax for upgrading monitor and boot images
on the management module**

Command syntax	Description
copy tftp flash <TFTP-server-ip-addr> <image-name> **mon**	Copies the latest monitor and boot images from the TFTP server to flash.
copy tftp flash <TFTP-server-ip-addr> <image-name> **boot**	Copies the latest boot images from the TFTP server to flash.
copy tftp flash <TFTP-server-ip-addr> <image-name> **mon copy-boot**	Copies the latest monitor and boot images from the TFTP server to flash.

For example, to copy the management module boot and monitor image from TFTP server 10.10.12.12, enter

```
BigIron RX# copy tftp flash 10.10.12.12 rmb02703a.bin mon copy-boot
```

3. Verify that the new monitor and boot images have been successfully copied to flash or slot 1 or 2 by entering one of the following commands at the Privileged EXEC level of the CLI:

   • **show flash**

   • **dir /<path-name>/** (if the destination is slot 1 or 2)

   Check for the boot image, monitor image, and the date and time at which the new images were built.

4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process.

Upgrading the management module IronWare image

To upgrade the management module IronWare image (primary or secondary), you must perform the following steps:

1. Place the new IronWare image on a TFTP server to which the BigIron RX system has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new IronWare image from the TFTP server or a flash card in slot 1 or 2 to the management module's code flash or a flash card in slot 1 or 2.

    To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI:

    *   **copy tftp flash** <TFTP-server-ip-addr> <image-name> **primary | secondary**

    *   **copy tftp slot1 | slot2** <TFTP-server-ip-addr> <image-name> **primary | secondary**

    *   **copy slot1 | slot2 flash** <image-name> **primary | secondary**

    *   **copy slot1 | slot2 slot1 | slot2** <image-name> <dest-name>

    For example, to copy the management module's Ironware image from TFTP server 10.10.12.12, enter

    ```
    BigIron RX# copy tftp flash 10.10.12.12 rmpr02703a.bin primary
    ```

3. Verify that the new IronWare image has been successfully copied to the specified destination by entering one of the following commands at the Privileged EXEC level of the CLI:

    *   **show flash** (if the destination was code flash)

    *   **dir /<path-name>/** (if the destination was slot 1 or 2)

    Check for the primary or secondary image and the date and time that it was placed in the directory.

4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process. For more information, see Rebooting the management module.

Upgrading the interface module monitor and boot images

We recommend that you perform this upgrade procedure from a PC or terminal that is directly connected to the management module Console port. You can also perform this procedure using a Telnet or SSHv2 session.

To upgrade monitor and boot images simultaneously for an interface, perform the following steps:

1. Place the new monitor and boot images on a TFTP server to which the BigIron RX system has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new monitor and boot images to the BigIron RX. Enter one of the following commands at the Privileged EXEC level of the CLI (example: BigIron RX#):

**Command syntax for upgrading the monitor and boot images
on the interface module**

Command syntax	Description
copy tftp lp <TFTP-server-ip-addr> <image-name>**mon all** | <slot-number>	Copies the latest monitor image from the TFTP server to all interface modules or to the specified interface module (slot-number).
copy tftp lp <TFTP-server-ip-addr> <image-name>**mon copy-boot all** | <slot-number>	Copies the latest monitor and boot images from the TFTP server to all interface modules or to the specified interface module (slot-number).

For example, to copy the interface module's boot and monitor image from TFTP server 10.10.12.12, enter

```
BigIron RX# copy tftp lp 10.10.12.12 rlb02703.bin mon all
```

3. Verify that the new images were successfully copied to code flash by entering the following command at the Privileged EXEC level of the CLI:

   • **show flash**

   Check for the monitor image, boot image, and the date and time at which the new images were built.

4. If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process. For more information, see Rebooting the management module.

Upgrading the IronWare image on the interface module

To upgrade the IronWare image (primary or secondary) on all interface modules or an interface module in a specified chassis slot, you must perform the following steps:

1. Place the new IronWare image on a TFTP server to which the BigIron RX system has access or on a PCMCIA flash card inserted in slot 1 or 2.

2. Copy the new IronWare image from the TFTP server or a flash card in slot 1 or 2 to all interface modules or an interface module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (example: BigIron RX#):

   • **copy tftp lp** <TFTP-server-ip-addr> <image-name> **primary | secondary all**

   • **copy tftp lp** <TFTP-server-ip-addr> <image-name> **primary | secondary** <chassis-slot-number>

   • **copy slot1 | slot2 lp** <image-name> **primary | secondary all**

   • **copy slot1 | slot2 lp** <image-name> **primary | secondary** <chassis-slot-number>

   For example, to copy the interface module IronWare image from TFTP server 10.10.12.12, enter

   ```
   BigIron RX# copy tftp lp 10.10.12.12 rlp02703a.bin primary all
   ```

> **NOTE:** If you copy the new IronWare image to all interface modules using the **all** keyword, the management module makes a copy of the image (called lp-primary-0 or lp-secondary-0) and stores it in its code flash, thereby synchronizing the new IronWare image on both the interface and management modules.
>
> If you copy the new IronWare image to a specified chassis slot, the management module does not make a copy of the image or store it. In this case, the new IronWare image on the interface module is unsynchronized or different from the IronWare image on the management module.
>
> For more information about synchronizing the new IronWare image or retaining unsynchronized versions of the IronWare image on the interface and management modules, refer to the section Rebooting the management module.

3. Verify that the new IronWare image has been successfully copied by entering the following command at any level of the CLI:

    ```
    BigIron RX# show flash
    ```

    Check for the IronWare image and the date and time at which the image was built.

If you want to upgrade other software images, go to the appropriate upgrade section for information. If you have completed upgrading the software images, you must reboot the management module to complete the upgrade process. For more information, see Rebooting the management module.

Upgrading MBRIDGE FPGA on the management module

BigIron RX management modules contain an upgradable FPGA images called MBRIDGE and SBRIDGE. The MBRIDGE and SBRIDGE image installed must be compatible with the software version you are running on the BigIron RX.

The following table describes the MBRIDGE FPGA versions required for the 02.7.03 versions.

MBRIDGE versions required per software version

Software image installed on BigIron RX	Current MBRIDGE image		Interface module
02.4.00	14		MP (Management Module)
02.4.00a	14		MP (Management Module)
02.4.00b	18		MP (Management Module)
02.4.00c	18		MP (Management Module)
02.4.00d	18		MP (Management Module)
02.4.00e	18		MP (Management Module)
02.4.00f	21		MP (Management Module)
02.4.00g	21		MP (Management Module)
02.5.00	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	20 20	MP (Management Module)
02.5.00a through	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)

Software image installed on BigIron RX	Current MBRIDGE image		Interface module
02.5.00f			
02.6.00a through 02.6.00c	BigIron RX-16/8/4 BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.00	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.01	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.01a through 02.7.01b	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.02	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.02a through 02.7.02h	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
02.7.03 through 02.7.03a	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)

Switch Fabric module FPGA versions required per software version (BigIron RX-32)

Software image installed on BigIron RX	FPGA image	Compatible FPGA version
02.5.00	SBRIDGE	6
02.5.00a through 02.5.00j	SBRIDGE	6
02.6.00	SBRIDGE	6
02.6.00a through 02.6.00e	SBRIDGE	6
02.7.00	SBRIDGE	6
02.7.01	SBRIDGE	6
02.7.01a through 02.7.01b	SBRIDGE	6
02.7.02	SBRIDGE	6
02.7.02a through 02.7.02h	SBRIDGE	6
02.7.03 through 02.7.03a	SBRIDGE	6

To upgrade the MBRIDGE FPGA image on a BigIron RX management module, you must perform the following general steps:

1. Determine the versions of the images currently installed on the BigIron RX management module using the **show version** command.

2. Place the new MBRIDGE FPGA image on a TFTP server to which the BigIron RX system has access or on a PCMCIA flash card inserted in slot 1 or 2.

3. Copy the MBRIDGE FPGA image from the TFTP server or a flash card in slot 1 or 2 to all management modules or a management module in a specified chassis slot. To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (example: BigIron RX#):

    • **copy tftp mbridge** <TFTP-server-ip-addr> <image-name> **MBRIDGE**

    • **copy slot1 | slot2 mbridge** <image-name> **MBRIDGE**

4. After the MBRIDGE upgrade is complete, the management module must be reloaded.

5. Verify that the MBRIDGE image(s) have been successfully copied to the specified interface module(s) by entering the following command at any level of the CLI:

    • **show version**

Check for the MBRIDGE image version numbers in the output. See MBRIDGE.

Rebooting the management module

After upgrading one or more software images on the management or interface module, you must reboot the management module. After the management module reboots, it in turn reboots the interface modules.

To reboot the management module, enter one of the following commands:

• **reload** (this command boots from the default boot source, which is the primary code flash)

• **boot system flash primary | secondary**

During the management module reboot, the following synchronization events occur:

• If you have a standby management module, the active management module compares the standby module's monitor, primary, and secondary images to its own. If you have updated these images on the active module, the active module automatically synchronizes the standby module's images with its own.

• If you copied the primary and/or secondary IronWare image to all interface modules using the **copy** command with the **all** keyword, the management module made a copy of the image and stored it in its code flash under the names lp-primary-0 or lp-secondary-0. By default, the BigIron RX system checks the interface modules' IronWare images, which reside in the code flash of the interface modules and the management module to make sure they are the same in both locations. (These IronWare images are stored on the management module only and are not run by the management or interface modules.) If the IronWare images on the interface and management modules are different, the system prompts you to do the following:

    o If you want to update the IronWare images in the interface module's code flash with the images in the management module's code flash, enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

    o If you want to retain the IronWare images in the interface module's code flash, enter the **lp cont-boot no-sync <slot-number>** command at the Privileged EXEC prompt.

After the management module finishes booting, do the following:

- Enter the **show module** command at any CLI level, and verify that the status of all interface modules is CARD_STATE_UP.

- Enter the **show version** command at any CLI level, and verify that all management and interface modules are running the new software image version.

If you find that an interface module is in a waiting state or is running an older software image, then you may have forgotten to enter the **lp cont-boot sync <slot-number>** command at the Privileged EXEC prompt.

You also need to upgrade the MBRIDGE FPGA on the management module.

Regenerating SSH v2 crypto key

If you are using SSH v2, you must clear the crypto key using the **crypto key zeroize** command after you upgrade from any release 02.2.01 and later. Then, regenerate a new crypto key using the **crypto key generate** command.

Hitless Layer 2 OS Upgrade

Hitless OS upgrades are supported for Layer 2 switching and Layer 2 protocols only. See the Upgrading Software Images and Configuration Files chapter in the *BigIron RX Installation Guide* for additional information. The hitless OS Layer 2 upgrade allows for upgrading the software in a system between two patch releases of the operating system, which support this functionality and have compatible data structures. A hitless OS Layer 2 downgrade may also be supported if the current and target code releases have compatible data structures.

Note: Hitless OS upgrade is not supported between major releases. It is supported only within a release. For example, Hitless OS Upgrade is available when upgrading from software release 02.7.00a to 02.7.00b. It is not available when upgrading from software release 02.6.00 to 02.7.00.

From time to time, it may become necessary when enhancing the software or adding new features to change or add data structures making releases incompatible. In these cases, an upgrade or downgrade will not be hitless, and will fall back to using the regular Brocade upgrade process – relying on fast reboot.

When performing a hitless O/S Layer 2 upgrade or downgrade, use the following guidance:

- Hitless O/S Layer 2 upgrade or downgrade is not supported in 2.3.00 or earlier.

- Hitless O/S Layer 2 upgrade support is in 2.3.00a and higher patch releases (unless indicated otherwise in the target software's release notes).

- Hitless upgrade maintains forwarding states and control plane functionality of the active software from which you are upgrading (i.e. 2.3.00a to 2.3.00d would only maintain the functionality supported by 2.3.00a).

- Hitless downgrades are recommended only between compatible patch releases of a feature release such as between 2.3.00b to 2.3.00a (to ensure the higher release has no conflicting functional enhancements that do not exist in the lower release).

- Due to the PBIF change introduced in patch release version 02.3.00e and version 02.3.00f, users cannot perform hitless upgrades from earlier 02.3.00 versions or 02.3.00g or higher versions. For information on Hitless Upgrades refer to the "Hitless OS Upgrade" section in the BigIron RX Installation Guide.

- Due to Internal changes introduced in patch release version 02.4.00d ,hitless upgrade is not supported onto   02.4.00b and hitless downgrade is not supported from 02.4.00d.

- The Hitless upgrade feature is not supported on release 02.5.00b to 02.5.00c for the BigIron RX-32 only. It is supported on all other BigIron RX devices.

Using this feature, you can upgrade the Multi-Service IronWare software without a loss of service or disruption in the following supported functions and protocols:

- All ports and links remain operational

- TOS-based QoS

- Layer-2 Switching

- Layer-2 Protocols:

    - MRP

    - STP

    - VSRP

    - RSTP

    - MSTP

Considerations when using the Hitless Layer 2 OS Upgrade feature

Consider the following when using the Hitless Layer 2 OS Upgrade feature:

- You must have both active and standby management modules installed to use this feature.

- To avoid any disruptions of Layer-3 traffic to OSPF or BGP routes, the switch must be configured with OSPF Graceful Restart and BGP Graceful Restart features. In addition, the device's OSFP neighbors must have OSPF Graceful Restart Helper enabled.

The total time it takes for the hitless upgrade process to finish varies between approximately 1 and 10 minutes. This depends on the size of the MAC table, the number of OSPF and BGP neighbors and the size of the routing table. Switch configuration is unavailable during the entire hitless upgrade process. The message "**---SW Upgrade In Progress - Please Wait---**" is printed at the console when configuration is attempted. Operational command of the switch is allowed during the upgrade process.

- The active management module changes from the initial active management module to the standby management module during the hitless upgrade process. This makes it necessary to have a connection to the console interface on both management modules.

- Upon being reset, the management and interface module CPUs are unable to send and receive any packets. Once the management and interface modules are up and running, their CPUs are able to send and receive packets, even before the hitless upgrade process is complete.

- Switch configuration is not allowed to be changed during the entire hitless upgrade process.

- System-max parameter changes or other configuration changes that require a system reload such as "cam-mode" and cam-profile" changes do not take effect upon hitless upgrade.

- FPGA images cannot be upgraded using the hitless upgrade process.

- This feature cannot be used to downgrade an image to an older major version than the version that the device is currently running.

IronWare Software Release 02.7.03a for Brocade BigIron RX Series Swtches

- If there are protocol dependencies between neighboring nodes, it's recommended that only each node is upgraded: one node at a time.

- After hitless upgrade, the BigIron RX switch will still have the same running configuration as it does before the upgrade. A configuration that is not saved before hitless reload is not removed and the existing startup configuration does not take effect. This behavior is the same as displayed by the management module switchover feature.

The Hitless OS Layer 2 software process

Hitless OS Layer 2 upgrade of Multi-Service IronWare software is performed in the following steps.

- Version 02.3.00 or later of the Multi-Service IronWare software is installed in flash memory to the primary and secondary image on the active and standby management modules and interface modules.

- The **hitless-reload** command is executed on the active management module.

- The hitless upgrade process is begun on the active management module which initiates the upgrade process on the standby management module.

- The standby management module is reset.

- The active management module is reset and the standby management module assumes control as the active module.

- Active console control is lost to the previously active management module as it becomes the standby management module.

- The active management module initiates the upgrade process on all interface modules.

- The switch is now operating on the new Multi-Service IronWare software. The management module that was initially configured as the standby management module is now the active management module and the management module that was initially configured as the active management module is now the standby.

Management module (MP) and Interface Module (LP) Hitless Upgrade Process provides a detailed diagram of the Hitless reload process.

Figure 1   Management module (MP) and Interface Module (LP) Hitless Upgrade Process
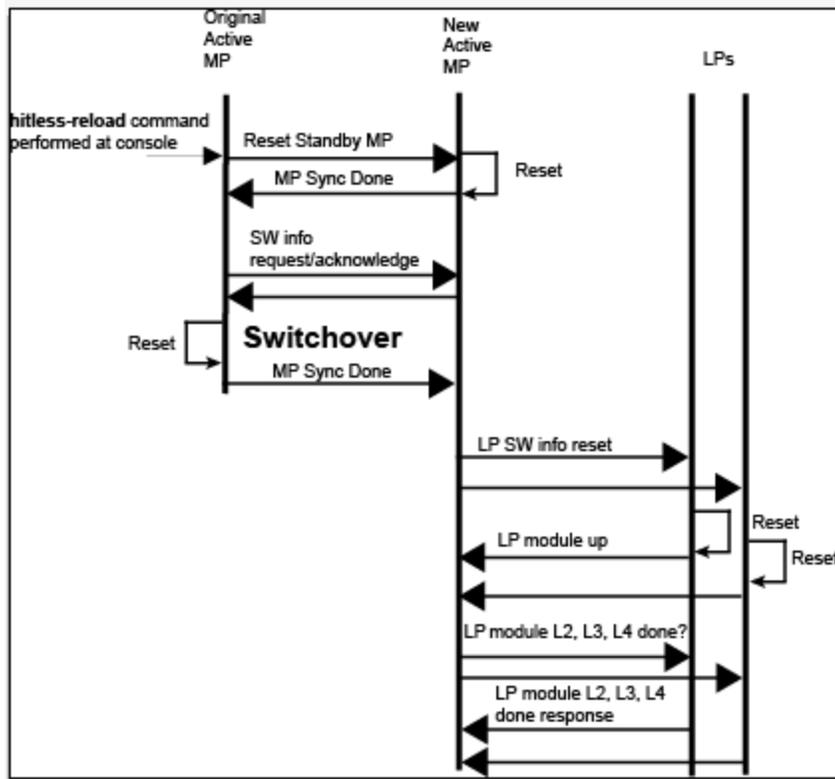
Performing a Hitless Layer 2 OS software upgrade

To perform a hitless Layer 2 OS software upgrade, you must perform the following tasks:

- Copy version 02.3.00 or later of the Multi-Service IronWare software to the primary and secondary image on both the active and standby management modules and interface modules.

- Setup a console connection to both the active and standby management modules. These connections can be through a telnet, SSH, or serial console session.

- Type the **hitless-reload** command at the console of the active management module.

Loading the Multi-Service IronWare software onto the switch

Hitless Layer 2 OS upgrade loads from the primary and secondary images on the Management modules. The first step in performing a hitless Layer 2 OS upgrade is to copy the version 02.3.00 or later images into the flash memory of the active and standby management modules.

For instructions for copying these files, see Upgrading the management module monitor and boot images and Upgrading the management module IronWare image.

Setting up consoles

Hitless Layer 2 OS upgrade is executed at the active management module. During the process of upgrading the image, control of the switch is shifted to the standby management module. For this reason, you need to have management sessions enabled on both the active and the standby management modules. When the reload is complete, the management module that was in the standby condition at the beginning will be in the active state. If you want the original management module to be active, you must manually

fail-over control to it.

Executing the Hitless upgrade command

To begin the process of a hitless upgrade, use the following command:

```
BigIron RX(config)# hitless-reload mp primary lp primary
```

Syntax: hitless-reload mp [primary | secondary] lp [primary | secondary]

The **mp** parameter specifies that the management module will be reloaded with either the **primary** or **secondary** image as directed.

The **lp** parameter specifies that the interface module will be reloaded with either the **primary** or **secondary** image as directed.

Verify the new software image

Enter the **show version** command at any CLI level, and verify that all management and interface modules are running the new software image version.

Technical support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

General Information

- Technical Support contract number, if applicable

- Switch model

- Switch operating system version

- Error numbers and messages received

- Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions

- Description of any troubleshooting steps already performed and the results

- Switch Serial Number

Getting Help or Reporting Errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Brocade using one of the following options.

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the **Product Documentation** tab, then click on the link to the Knowledge Portal (KP) to find the latest document.

While in the Knowledge Portal, you can click on **Cases > Create a New Ticket** to report an error. Make sure you specify the document title in the ticket description.

IronWare Software Release 02.7.03a for Brocade BigIron RX Series Swtches

E-mail and telephone access

Go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Additional resources

Below are some additional publications you can reference to find more information on the products supported in this software release.

Additional publications

Title	Contents
Brocade BigIron RX Series Installation Guide	• Product Overview • Installation • Product Management • Hardware Maintenance and Replacement • Air filters • Fiber optic connectors • Replaceable modules • AC Power supply • Fans • Software Upgrades • Hardware Specifications • Regulatory Statements
BigIron RX Series Configuration Guide	Information on how to configure all the features in a BigIron RX Series switch.
Ironware MIB Reference	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
IronView® Network Manager User Guide	SNMP-based application for managing Brocade switches and switching routers.

Defects

NOTE: In the tables below, "Reported In Release" indicates the product and release that the defect was first identified. If the problem also appeared in other Brocade IP Products, the issue was addressed using the same defect ID.

Closed defects with code change in Multi-Service IronWare R02.7.03a.

Defect ID:	DEFECT000316902	Technical Severity:	High
Summary:	An LSA with a higher metric can prevent the route installation of an LSA which has a lower metric and broadcast address LS ID.		
Symptom:	When a static route is added on one router, a route for the same network may disappear on another router.		
Probability:	High		
Feature:	OSPF	**Function:**	Redistribution
Reported In Release:	RX 02.7.00	**Service Request ID:**	260272

Defect ID:	DEFECT000317027	Technical Severity:	Medium
Summary:	Router sends duplicate multicast packets when IGMP Snooping and Sflow are enabled.		
Probability:	Medium		
Feature:	IPv4-MC IGMP	**Function:**	IGMPv1/v2 Protocol
Reported In Release:	RX 02.7.02	**Service Request ID:**	259119

Defect ID:	DEFECT000318055	Technical Severity:	Medium
Summary:	Removed ability to set temperature polling interval to zero using CLI.		
Probability:	High		
Feature:	SYSTEM	**Function:**	Temp sensor & Monitoring
Reported In Release:	RX 02.7.02	**Service Request ID:**	256590

Defect ID:	DEFECT000318432	Technical Severity:	Medium
Summary:	If "clock summer-time" is configured, then system reloads one hour later than the configured reload time using "reload at" command.		
Symptom:	After configuring "clock summer-time" the system reloads one hour later than the configured reload time when using the "reload at" command.		
Probability:	Low		
Feature:	SYSTEM	**Function:**	TIMER
Reported In Release:	RX 02.7.02	**Service Request ID:**	262013

Defect ID:	DEFECT000321237	Technical Severity:	Medium
Summary:	When a stub area is configured the 'show ip ospf border-router' command incorrectly displays the area value.		
Probability:	Medium		
Feature:	OSPF	**Function:**	show commands
Reported In Release:	RX 02.7.02	**Service Request ID:**	262838

Defect ID:	DEFECT000321390	Technical Severity:	Medium
Summary: ARP packets transiting through the router, tagged with VLAN ID 0 (Priority tag) are being dropped.			
Probability: High			
Feature: IPv4 Forwarding		**Function:** ARP	
Reported In Release: RX 02.7.03			

Defect ID:	DEFECT000322582	Technical Severity:	Medium
Summary: When a fan power supply write error occurs, an incorrect value of 31 may be displayed on the screen.			
Probability: Low			
Feature: SYSTEM		**Function:** Fan	
Reported In Release: RX 02.7.03		**Service Request ID:** 263334	

Defect ID:	DEFECT000323122	Technical Severity:	Low
Summary: When using a line password for telnet authentication, fewer commands than normal are available after leaving enable mode. This problem is unique to environments that have "aaa authentication login default line" configured.			
Symptom: When using a line password for telnet authentication, fewer commands than normal are available after leaving enable mode.			
Probability: High			
Feature: AAA		**Function:** Local Authentication	
Reported In Release: RX 02.7.03		**Service Request ID:** 263592	

Defect ID:	DEFECT000323269	Technical Severity:	High
Summary: Interface module may reload after 'show ip cache' command is executed.			
Symptom: Interface module may reload after 'show ip cache' command is entered on an Interface module which had run out of next-hop entries.			
Probability: Low			
Feature: CLI Infrastructure		**Function:** Parser Engine	
Reported In Release: RX 02.7.02		**Service Request ID:** 265696	

Defect ID:	DEFECT000323367	Technical Severity:	Medium
Summary: IP Cache-entry is not removed until either ARP entry is removed or IP Cache entry is cleared.			
Symptom: IP next-hop table may become full on the router.			
Probability: High			
Feature: IPv4 Forwarding		**Function:** Next Hop Table	
Reported In Release: RX 02.7.02		**Service Request ID:** 265521	

Defect ID:	DEFECT000324004	Technical Severity:	Medium
Summary: The interface level "ip arp-age" command is enhanced to selectively increase ARP-age for a particular IP interface.			
Symptom: ARP occurs every five minutes even though the ARP-age value is set much higher.			
Probability: Medium			
Feature: IPv4 Forwarding		**Function:** ARP	
Reported In Release: RX 02.7.02		**Service Request ID:** 265832	

Defect ID:	DEFECT000325553	Technical Severity:	Medium
Summary: In some cases wherein traffic ingresses on a LAG port, PIM needlessly reprograms a hardware entry leading to a small packet loss.			
Probability: Medium			
Feature: IPv4-MC PIM-SM Routing		**Function:** PROTOCOL	
Reported In Release: RX 02.7.02		**Service Request ID:** 267599	

Defect ID:	DEFECT000326324	Technical Severity:	Medium
Summary: Output from 'tag-type' command is truncated to 200 characters.			
Probability: High			
Feature: CLI Infrastructure		**Function:** Parser Engine	
Reported In Release: RX 02.7.03		**Service Request ID:** 267672	

Closed defects with code change in Multi-Service IronWare R02.7.03.

Defect ID:	DEFECT000271667	Technical Severity:	Medium
Summary: Line Modules may reload during multicast memory request because of memory corruption. Cannot reproduce.			
Symptom: Line modules may reload.			
Probability: Low			
Feature: IPv4-MC PIM-SM Routing		**Function:** PROTOCOL	
Reported In Release: RX 02.6.00		**Service Request ID:** 224751	

Defect ID:	DEFECT000271749	Technical Severity:	High
Summary: System reloads while processing while collecting task utilization information. Could not reproduce.			
Symptom: System reload			
Probability: Low			
Feature: OS		**Function:** OS	
Reported In Release: RX 02.5.00		**Service Request ID:** 226940	

Defect ID:	DEFECT000271873	Technical Severity:	Medium
Summary: The system may reload when formatting an invalid PCMCIA card.			
Symptom: System may reload			
Probability: Low			
Feature: SYSTEM		**Function:** Flash memory	
Reported In Release: RX 02.6.00		**Service Request ID:** 235167	

Defect ID:	DEFECT000271877	Technical Severity:	High
Summary: CPU session cache may erroneously match when identical packets arrive on different ve's			
Symptom: Clients are unable to get an IP address via DHCP.			
Probability: Medium			
Feature: ACL		**Function:** IPv4	
Reported In Release: RX 02.6.00		**Service Request ID:** 223618	

Defect ID:	DEFECT000271887	Technical Severity:	Medium
Summary: Line module stopped responding after issuing "show ip lpm count" command. Happens when ecmp routes are present.			
Symptom: Interface ports on the line module went into a down state. There was no crash.			
Probability: Medium			
Feature: SYSTEM		**Function:** Tiger HAL	
Reported In Release: RX 02.6.00		**Service Request ID:** 231524	

Defect ID:	DEFECT000271931	Technical Severity:	High
Summary: VRRP/STP flap when BGP session is reset (full Internet route table is withdrawn and updated)			
Symptom: VRRP flap is seen.			
Probability: Medium			
Feature: L2 Protocol		**Function:** VSRP1	
Reported In Release: RX 02.4.00		**Service Request ID:** 178709	

Defect ID:	DEFECT000272063	Technical Severity:	Medium
Summary: Broadcast traffic is CPU forwarded when enabling IP multicast active.			
Symptom: High CPU			
Probability: Medium			
Feature: IPv4-MC IGMP		**Function:** PERFORMANCE	
Reported In Release: RX 02.6.00		**Service Request ID:** 211954	

Defect ID:	DEFECT000272067	Technical Severity:	High
Summary: Need ability to resolve IPv6 addresses using IPv4 transport per the RFC 3596			
Symptom: RX cannot resolve IPv6 addresses through IPv4 DNS queries			
Probability: High			
Feature: DNS		**Function:** PROTOCOL	
Reported In Release: RX 02.7.00		**Service Request ID:** 215029	

Defect ID:	DEFECT000273160	Technical Severity:	Medium
Summary: IP syslog source-interface command not functioning			
Symptom: All of the logs to the syslog server are tagged with IP address of the interface where they come out.			
Workaround: downgrade to 2.6.00 tree			
Probability: Medium			
Feature: SYSLOG		**Function:** System Integration	
Reported In Release: RX 02.7.02		**Service Request ID:** 237819	

Defect ID:	DEFECT000273335	Technical Severity:	Medium
Summary: SNMP GET on ifSpeed not returning correct value when interface is in 1000-slave mode.			
Symptom: A Get request for ifSpeed returns a value of 0 when interface is in 1000-slave mode.			
Probability: High			
Feature: SYSTEM		**Function:** OPTICS	
Reported In Release: RX 02.7.02		**Service Request ID:** 237209	

Defect ID:	DEFECT000273671	Technical Severity:	High
Summary: When DHCP snooping is enabled and attached hosts with ARP entries of type 'dhcp' has a link go down and then up, the existing IP cache entries get set to drop traffic when the link goes down but does not get updated when the link comes back up.			
Symptom: Traffic may get dropped or 'blackholed' to certain hosts until a 'clear arp' is issued.			
Workaround: Workaround would be to disable dhcp snooping feature.			
Probability: High			
Feature: IPv4 Forwarding		**Function:** ARP	
Reported In Release: RX 02.7.02		**Service Request ID:** 236355	

Defect ID:	DEFECT000273769	Technical Severity:	Medium
Summary: Modifying an ACL may cause a reload.			
Symptom: System may reload			
Probability: Low			
Feature: ACL		**Function:** IPv4	
Reported In Release: RX 02.7.02		**Service Request ID:** 237740	

Defect ID:	DEFECT000274156	Technical Severity:	Medium
Summary: Command "show interface slot 0" may cause a system reset.			
Symptom: System may reload			
Probability: Medium			
Feature: CLI Infrastructure		**Function:** Parser Engine	
Reported In Release: RX 02.7.02		**Service Request ID:** 238294	

Defect ID:	DEFECT000275397	Technical Severity:	High
Summary: The RX may reload when parsing a configuration file with a large number of untagged ports on the same line.			
Symptom: System may reload			
Probability: Medium			
Feature: L2 Forwarding		**Function:** MAC Manager	
Reported In Release: RX 02.7.02		**Service Request ID:** 239259	

Defect ID:	DEFECT000278996	Technical Severity:	Medium
Summary: The Web-GUI shows switch fabrics in the wrong slot locations.			
Symptom: Web Manager does not display the correct slot order.			
Probability: High			
Feature: Web Management		**Function:** FRONT PANEL	
Reported In Release: RX 02.7.02		**Service Request ID:** 240600	

Defect ID:	DEFECT000278997	Technical Severity:	Critical
Summary: IPv6 mld snooping is not supported in RX. Turning ON "ipv6 multicast active" or "ipv6 multicast passive" will cause buffer leakage on LP. The following error message is a symptom of the problem. LP may eventually reset. "ITC warning: Message IP_RX_L2M			
Symptom: Line modules may shut down and the following errors may be reported: "ITC warning: Message IP_RX_L2MCAST6_ID (000b1014) received for app 00000025, with no handler registered"			
Probability: Low			
Feature: IPv6-MC Snooping VLANs		**Function:** CLI	
Reported In Release: RX 02.7.02		**Service Request ID:** 2408642	

Defect ID:	DEFECT000279003	Technical Severity:	Medium
Summary: The LED on the Web-GUI for the 24x1 Gig copper module is transposed between ports 1 and 2.			
Symptom: Incorrect LED status seen on the Web GUI.			
Probability: High			
Feature: Web Management		**Function:** FRONT PANEL	
Reported In Release: RX 02.7.02		**Service Request ID:** 240600	

Defect ID: DEFECT000279523	Technical Severity: Medium
Summary: The LED status on the Web-GUI LED for the 16x10GE module is transposed between the odd and even ports.	
Feature: Web Management	Function: FRONT PANEL
Reported In Release: RX 02.7.03	

Defect ID: DEFECT000279728	Technical Severity: Medium
Summary: Multicast traffic is flooded on all ports when IGMPv3 snooping enabled.	
Symptom: Multicast traffic is flooded on all ports.	
Probability: Medium	
Feature: IPv4 MC-Snooping (VLAN)	Function: IGMPv3 Snooping
Reported In Release: RX 02.7.02	Service Request ID: 240868

Defect ID: DEFECT000279953	Technical Severity: Medium
Summary: STP BPDUs may be dropped across the Q-in-Q link	
Probability: Medium	
Feature: L2 Protocol	Function: STP
Reported In Release: RX 02.7.02	Service Request ID: 238581

Defect ID: DEFECT000281680	Technical Severity: Medium
Summary: SNMP GET on The SNMPEngineTime does not return the correct system uptime.	
Symptom: SNMP GET on The SNMPEngineTime does not return the correct system uptime.	
Probability: Medium	
Feature: SNMP Management	Function: Trap/Notification
Reported In Release: RX 02.7.02	Service Request ID: 242084

Defect ID: DEFECT000281762	Technical Severity: Medium
Summary: IPv6 Traps are not sent if an IPv4 address is not configured on the XMR/MLX or RX.	
Symptom: Configure IPv4 address and then configure IPv6 address.	
Probability: Medium	
Feature: SNMP Management	Function: Trap/Notification
Reported In Release: RX 02.7.02	Service Request ID: 241172

Defect ID: DEFECT000281788	Technical Severity: Medium
Summary: Remove CLI command for packet logging. This feature is not supported on RX.	
Symptom: CLI command for packet logging is non-functional. This feature is not supported on RX.	
Probability: Low	
Feature: CLI Infrastructure	Function: Page Mode Display
Reported In Release: RX 02.7.02	Service Request ID: 241827

Defect ID: DEFECT000283672	Technical Severity: Medium
Summary: BGP speaker does not advertise update to origin AS	
Symptom: Customer wanted to advertise eBGP update received from a router in AS <N> to a different router in AS <N> . This design is supported on the MLX but is currently not available on the RX.	
Probability: High	
Feature: BGP	Function: BGPv4
Reported In Release: RX 02.7.02	Service Request ID: 243183

Defect ID:	DEFECT000284653	Technical Severity:	Medium
Summary:	Not able to set Extended IP ACL Protocol field to ESP(50) from SNMP		
Symptom:	Customer was trying to implement ACL to RX from INM but failed. Using CLI command the access list is added without any problem access-list 105 permit esp host 1.1.1.1 host 2.2.2.2		
Probability:	High		
Feature: SNMP Management		**Function:** IP Mib	
Reported In Release: RX 02.7.02		**Service Request ID:** 241185	

Defect ID:	DEFECT000286364	Technical Severity:	Medium
Summary:	Change gig auto negotiation behavior.		
Symptom:	Currently, between two gig fiber interfaces, when one side is configured with gig-default auto (default), the other side is gig-default neg-off, links show up at both sides. Default behavior will change to the side with neg-off configured shows link up and the side with auto configured shows link down. In addition: gig-default auto-full is added to switch back to the current behavior (none-default behavior after the code change).		
Probability:	Medium		
Feature: SYSTEM		**Function:** OPTICS	
Reported In Release: RX 02.7.02		**Service Request ID:** 242203	

Defect ID:	DEFECT000287890	Technical Severity:	Medium
Summary:	BGP "allowas-in" does not with confederation config		
Symptom:	BGP Routes received from peer with local AS (in as-path) are dropped even though "allowas-in" is used for that particular peer. We have observed this issue only when confederation is configured. Without confederation it works fine.		
Probability:	High		
Feature: BGP		**Function:** BGPv4	
Reported In Release: RX 02.7.00			

Defect ID:	DEFECT000288254	Technical Severity:	High
Summary:	Under "ipv6 router ospf", the "in" parameter after a "distribute-list prefix-list" isn't saved to the running config.		
Symptom:	Under "ipv6 router ospf", the "in" parameter after a "distribute-list prefix-list" isn't saved to the running config even though it is required when entering a "distribute-list prefix-list". As a result, the config is lost when the write mem command is issued and the device is reloaded.		
Probability:	High		
Feature: OSPFv3		**Function:** CONFIGURATION	
Reported In Release: RX 02.7.02		**Service Request ID:** 245558	

Defect ID:	DEFECT000288573	Technical Severity:	Medium
Summary:	LAG port name was only displayed up to 9 characters.		
Symptom:	LAG port names are being cutoff in the show lag output.		
Probability:	Medium		
Feature: Character I/O		**Function:** Character Handling	
Reported In Release: RX 02.7.02		**Service Request ID:** 244909	

Defect ID: DEFECT000290430	Technical Severity: Medium
Summary: When a port is removed from a LAG it gets stuck in blocking state.	
Symptom: If an up interface is added to a LAG, but the LAG is not deployed and then the interface is removed from the LAG. The interface could be left in blocking state.	
Probability: Low	
Feature: LAG	Function: LACP
Reported In Release: RX 02.7.02	Service Request ID: 238882

Defect ID: DEFECT000290641	Technical Severity: High
Summary: ARP sync may fail during high rate of IPC traffic	
Symptom: ARP entries may in certain situations be higher on Linecard resulting in "out of sync" condition and 'blackhole' of traffic.	
Workaround: Hosts can be pinged from MP in order to trigger arp sync of entry	
Probability: Medium	
Feature: IPv4 Forwarding	Function: ARP
Reported In Release: RX 02.7.02	

Defect ID: DEFECT000298275	Technical Severity: High
Summary: Interface module reloads when add/remove interface rate-limit command	
Symptom: Interface module reloads.	
Probability: Medium	
Feature: ACL	Function: IPv4
Reported In Release: RX 02.4.00	Service Request ID: 246870

Defect ID: DEFECT000299727	Technical Severity: Medium
Summary: Show redundancy endtime display may be corrupted	
Symptom: Show redundancy endtime display corrupted	
Probability: Low	
Feature: SYSTEM	Function: Hitless failover
Reported In Release: RX 02.7.02	Service Request ID: 249289

Defect ID: DEFECT000299851	Technical Severity: High
Summary: Create new VLAN command gets insufficient FIDs for VLAN creation error	
Symptom: Multicast MAC entries don't age in hardware and over time FIDs resource is exhausted. When configuring new VLAN, the following error occurs RX(config)#vlan 3100 n error - insufficient fids available for vlan creation	
Workaround: If the user executes "clear ip multicast all" the FIDs will be reclaimed.	
Probability: Low	
Feature: IPv4 MC-Snooping (VLAN)	Function: IGMP Snooping
Reported In Release: RX 02.7.02	Service Request ID: 247249

Defect ID: DEFECT000300236	Technical Severity: Medium
Summary: RX only sends SNMPv1 traps, and there is no way to generate traps in SNMPv2 or v3.	
Symptom: Unable to generate traps in SNMPv2 or v3.	
Probability: Medium	
Feature: SNMP Management	Function: Trap/Notification
Reported In Release: RX 02.7.02	Service Request ID: 249438

Defect ID:	DEFECT000301863	Technical Severity:	High
Summary: An OSPF route with metric of 65535 is not installed in the routing table.			
Symptom: Using the configuration 'auto-cost reference-bandwidth 100000' will prevent routes from a GRE tunnel interface from being installed.			
Workaround: Remove the auto-cost reference-bandwidth 100000 or set the cost on the GRE tunnel interface.			
Probability: High			
Feature: OSPF		**Function:** PROTOCOL	
Reported In Release: RX 02.7.02		**Service Request ID:** 248796	

Defect ID:	DEFECT000302010	Technical Severity:	Medium
Summary: Inserted "0" to ipv6 prefix-list for fe80::/			
Symptom: When IPv6 prefix list was created, only fe80::/ prefix list automatically inserted "0" to running-config.			
Probability: High			
Feature: IPV6		**Function:** Prefix-list	
Reported In Release: RX 02.7.02		**Service Request ID:** 246057	

Defect ID:	DEFECT000302184	Technical Severity:	Medium
Summary: System reloads due to an incorrect Management module sync message			
Probability: Low			
Feature: SYSTEM		**Function:** Event Manager	
Reported In Release: RX 02.6.00		**Service Request ID:** 251711	

Defect ID:	DEFECT000302396	Technical Severity:	Medium
Summary: The RADIUS configuration is missing the auth-port keyword for ipv6 which can result in the command not getting parsed correctly on reload.			
Symptom: The RADIUS configuration is missing the auth-port keyword for IPv6 which can result in the command not getting parsed correctly on reload. telnet@XMR13(config)#radius-server host ipv6 fe80::2 ? DECIMAL Number			
Workaround: Need to re-enter radius-server CLI command every time after reload.			
Probability: High			
Feature: AAA		**Function:** RADIUS Authentication	
Reported In Release: RX 02.7.02		**Service Request ID:** 247801	

Defect ID:	DEFECT000303316	Technical Severity:	Medium
Summary: The router may reload when issuing the "show media" command.			
Symptom: Reload			
Probability: Medium			
Feature: SYSTEM		**Function:** I2C	
Reported In Release: RX 02.7.02		**Service Request ID:** 251305	

Defect ID:	DEFECT000303782	Technical Severity:	High
Summary: High CPU may occur when IGMP & PIM is configured.			
Symptom: Running PIM on multiple VLANs that have a large numbers of ports, the following message may be seen below every igmp query interval. "[mcast] ip_tx's Q is Full - max 65536, 65536, current 65512, 0"			
Probability: Medium			
Feature: IPv4-MC IGMP		**Function:** SCALABILITY	
Reported In Release: RX 02.7.02		**Service Request ID:** 249377	

Defect ID: DEFECT000305721	Technical Severity: Medium
Summary: OSPF interface cannot be established between a VE interface on 16x10G linecard. This was seen when the 16x10G card is in an RX-4 system.	
Symptom: Unable to for a OSPF adjacency.	
Probability: High	
Feature: OSPF	**Function:** PROTOCOL
Reported In Release: RX 02.7.02	**Service Request ID:** 251533

Defect ID: DEFECT000306096	Technical Severity: High
Summary: With Multicast enabled, traffic may stop forwarding due to buffer depletion.	
Symptom: Protocols went down due to buffer depletion.	
Probability: Low	
Feature: IPv4-MC PIM-SM Routing	**Function:** SCALABILITY
Reported In Release: RX 02.7.02	**Service Request ID:** 249142

Defect ID: DEFECT000306310	Technical Severity: Medium
Summary: Console message "incomplete command" may be seen when configuring a remark parameter on named access-lists.	
Symptom: An error message is seen when configuring a ACL.	
Probability: Low	
Feature: ACL	**Function:** IPv4
Reported In Release: RX 02.7.02	**Service Request ID:** 251509

Defect ID: DEFECT000306574	Technical Severity: Medium
Summary: A static RP ACL fails to map if one of the RP ACLs is not defined.	
Symptom: ACL is not working correctly.	
Probability: Medium	
Feature: IPv4-MC PIM-SM Routing	**Function:** Static RP
Reported In Release: RX 02.7.02	**Service Request ID:** 255479

Defect ID: DEFECT000308240	Technical Severity: High
Summary: An Interface module may reload if a trunk port with multicast boundary flaps.	
Symptom: Interface module reloads.	
Probability: Low	
Feature: IPv4-MC PIM-SM Routing	**Function:** Multicast Boundary- TTL Threshold
Reported In Release: RX 02.7.02	**Service Request ID:** 255504

Defect ID: DEFECT000308974	Technical Severity: Medium
Summary: When a LAG is configured with a combination of 16x10G ports and 4x10G ports on the same chassis some protocols fail.	
Symptom: LAG across ports from both 16x10 and 4x10 line cards may stop forwarding traffic after some time.	
Workaround: Don't assign non 16x10 ports to a 16x10 LAG.	
Probability: Low	
Feature: LAG	**Function:** Static
Reported In Release: RX 02.7.02	**Service Request ID:** 251681

Defect ID:	DEFECT000310404	Technical Severity:	Critical
Summary: The management module may reload when issuing the command 'sh stat brief lag' from telnet session.			
Symptom: Reload			
Probability: Low			
Feature: LAG		**Function:** LACP	
Reported In Release: RX 02.7.02		**Service Request ID:** 255300	

Defect ID:	DEFECT000310529	Technical Severity:	High
Summary: An Interface module may reload when a new L2 multicast stream is received.			
Symptom: Interface module may reload			
Probability: Low			
Feature: IPv4 MC-Snooping (VLAN)		**Function:** IGMP Snooping	
Reported In Release: RX 02.7.02			