Multi-Service IronWare Software Release 02.8.00a for Brocade BigIron RX Series Switches

Release Notes v1.0

August 12, 2011

Document History

Document Title	Summary of Changes	Publication Date
Multi-Service IronWare Software Release 02.8.00a for Brocade BigIron RX Series Switches Release Notes v1.0	Release 02.8.00a	August 2011

Contents

Supported devices for Multi-Service IronWare Release 02.8.00a

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 this 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

The enhancements for the Multi-Service IronWare software are descibed in this section.

Release 02.8.00a

BigIron RX device does not properly restrict packets sent with a source port of 179. Port 179 is commonly used for Border Gateway Protocol (BGP) communication. These packets are allowed through the system. This has been reported by US-CERT http://www.kb.cert.org/vuls/id/853246 (Defect 000355173).

In Release 02.8.00a of the Multi-Service IronWare software, a new CLI command, hw-opt bgp | bfd, was added to disable internal ACLs for BGP and BFD.

To deny BGP traffic on the interface 1/15, enter the following commands.

```
BigIron RX(config)# interface ethernet 1/15
BigIron RX(config-if-e10000-1/15)# enable
BigIron RX(config-if-e10000-1/15)# hw-opt bgp
BigIron RX(config-if-e10000-1/15)# exit
```

Syntax: hw-opt bgp | bfd

The **bgp** parameter disables prioritization of BGP packets.

The **bfd** parameter disables prioritization of BFD packets.

Release 02.8.00

The following table lists the enhancements for the release 2.8.00.

Table 1: Enhancements for Release 02.8.00

Enhancement	Description	Described in
Multi-device Port Authentication	Multi-device port authentication is now supported on the BigIron RX tagged and untagged ports.	Book: BigIron RX Series Configuration Guide Chapter: Configuring Multi-Device Port Authentication Section: How multi-device port authentication works
Enhanced show arp command to display ARP entries for a particular virtual interface (VE)	The show arp command has been enhanced to support the display of ARP entries for the specified virtual interface (VE).	Book: BigIron RX Series Configuration Guide Chapter: Configuring IP Section: Displaying the ARP cache
Enhanced command to display STP, RSTP, and MSTP information for a particular Ethernet interface	The show xstp command is newly added. It displays STP, RSTP, and MSTP protocol information for a particular Ethernet interface.	Book: BigIron RX Series Configuration Guide Chapter: Configuring Spanning Tree Protocol Section: Displaying STP information for the specified Ethernet interface Chapter: Configuring Rapid Spanning Tree Protocol Section: Displaying RSTP information for the specified Ethernet interface Chapter: Multiple Spanning Tree Protocol (MSTP) 802.1s Section: Displaying MSTP information for the specified Ethernet interface
Copy software image from a flash card to the flash memory	In Release 02.8.00 of the Multi-Service IronWare software, a new copy command has been added to copy the software image from a flash card to the flash memory.	Book: BigIron RX Series Configuration Guide Chapter: Using a Redundant Management Module Section: Copying software image from a flash card to the flash memory
Continuous System Monitoring (Sysmon)	Continuous system monitoring (Sysmon) is implemented in BigIron RX to monitor the overall system operation. It monitors different system components of a router or a switch to determine if those components are operating correctly.	Book: BigIron RX Series Configuration Guide Chapter: Continuous System Monitor

Enhancement	Description	Described in
Enhancement in ACL Support	Brocade RX devices now support IPv4 and IPv6 ACLs on the same interface	Book: BigIron RX Series Configuration Guide

Feature support

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

Supported features

The following table lists the features supported on the BigIron RX switches.

Table 2: Supported features for Release 02.8.00

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	Allows the logging of all valid CLI commands from each user session into the system log.
• 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
• Management Options	Serial and Telnet access to industry-standard Command Line Interface (CLI) Secure Shell (SSH) version 2 (v2) TFTP Web-based GUI SNMP (Version 1,Version 2, and Version 3) IronView Network Manager

Category	Feature description
• Security	AAA Authentication Local passwords RADIUS SSHv2 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
• 802.1q	see VLANs, below
• 802.1s	Multiple Spanning Tree Protocol (MSTP)
• 802.1w	Rapid Spanning Tree Protocol (RSTP)

Category	Feature description
• 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	Provides automatic failover from the active management module to the standby management module without interrupting operation of any interface modules in the chassis.
• Layer 2 IGMP Snooping	The BigIron RX supports 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	• The BigIron RX supports 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+

Category	Feature description
• IPv6 Multicast	PIM-SM
	MLD

Unsupported features

The following features are not supported in software release 02.8.00 on BigIron RX:

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

Software image files for Multi-Service IronWare Release 02.8.00a

The following software image files are available for Multi-Service IronWare Release 02.8.00a for the BigIron RX Series switches.

Table 3: Software image files

Module	Image type	Image name
Unified Image	N/A	rx02800a.bin
Management Module	Boot and Monitor	rmb02800a.bin
	IronWare	rmpr02800a.bin
BigIron RX-4, BigIron RX-8, and BigIron RX-16	FPGA	mbridge.xsvf

Module	Image type	Image name
BigIron RX-32		mbridge32.xsvf
Interface Module	Boot and Monitor	rlb02800a.bin
	IronWare	rlp02800a.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 based on version upgrade – 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.

- Displaying the version information – This sub-section describes the commands that allow you to determine the contents of the flash memory in the BigIron RX Series switch 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 Series switches monitor and Multi-Service IronWare 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 need to upgrade Unified Multi-Service IronWare image. The boot image will need to be upgraded only if it is specifically mentioned 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 procedure for upgrading the BigIron RX Series switches boot image, 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# show version
========================================================================
HW: BigIron RX Router
BigIron RX-8 CHASSIS (Serial #: SA35065043, Part #: 31549-000B)
RX-BI-SFM3 Switch Fabric Module 1 (Serial #: SA43080812, Part #: 35523-201B)
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 #: SA42081175, Part #: 35523-201B)
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 #: SA42081159, Part #: 35523-201B)
FE 1: Type fe200, Version 2
FE 2: Type fe200, Version 2
FE 3: Type fe200, Version 2
========================================================================
SL M2: RX-BI-MR Management Module Active (Serial #: SA11080037, Part #: 35524-
102A):
Boot     : Version 2.8.0T145 Copyright (c) 1996-2010 Brocade Communications
Systems, Inc.
Compiled on Apr 20 2011 at 01:07:14 labeled as rmb02800
 (439602 bytes) from boot flash
Monitor: Version 2.8.0T145 Copyright (c) 1996-2010 Brocade Communications Systems,
Inc.
Compiled on Apr 20 2011 at 01:07:14 labeled as rmb02800
 (439633 bytes) from code flash
IronWare: Version 2.8.0T143 Copyright (c) 1996-2010 Brocade Communications Systems,
Inc.
Compiled on Apr 20 2011 at 01:12:50 labeled as rmpr02800
 (4550480 bytes) from Primary
Board ID: 00 MBRIDGE Revisions: 21
916 MHz Power PC processor (version 8003/0101) 166 MHz bus
512 KB Boot Flash (AM29LV040B), 32 MB Code Flash (MT28F128J3)
1024 MB DRAM
```

```
Active Management uptime is 2 minutes 2 seconds
==========================================================================
SL 1: RX-BI-24C 24-port 1 GbE Copper Module (Serial #: SA51050944, Part #: 31521-
001D)
Boot     : Version 2.7.3T155 Copyright (c) 1996-2010 Brocade Communications
Systems, Inc.
Compiled on Apr 20 2011 at 15:09:22 labeled as rlb02800
 (307473 bytes) from boot flash
Monitor: Version 2.8.0T155 Copyright (c) 1996-2010 Brocade Communications Systems,
Inc.
Compiled on Apr 20 2011 at 01:07:02 labeled as rlb02800b
 (307473 bytes) from code flash
IronWare: Version 2.8.0T157 Copyright (c) 1996-2010 Brocade Communications Systems,
Inc.
Compiled on Apr 20 2011 at 01:16:26 labeled as rlp02800
 (2340308 bytes) from Primary
FAP 1 version: 2
FAP 2 version: 2
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 59 seconds
..All show version done
```

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

Different image information

The following sections describe the various software images for the management module and interface module.

Management Modules

The following table describes the various software images for the management module.

Table 4: Software image files for management modules

Field	Description
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.

Field	Description
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

The following table describes the various software images for the interface module.

Table 5: Software image files for interface module

Field	Description
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

Field	Description
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 switch fabric module for the BigIron RX-32 .

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 Multi-Service IronWare image of both management and interface modules. You can use the following command 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 (rx02800a.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 rx02800a.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 Multi-Service 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 is 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 rx02800a.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 do not 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 monitor and boot images on the management module

To upgrade the monitor and boot images on the management module, 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 slot 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 (For example: `BigIron RX#`):

**Table 6: 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 image 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 the following command.

```
BigIron RX# copy tftp flash 10.10.12.12 rmb02800a.bin mon copy-boot
```

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

```
BigIron RX# show flash
```

```
BigIron RX# dir /<path-name>/
```
(if the destination was slot 1 or slot 2) and 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 IronWare image on the management module

To upgrade the IronWare image (primary or secondary) on the management module, 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 slot 2.

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

    To perform this step, enter one of the following commands at the Privileged EXEC level of the CLI (For example: `BigIron RX#`):

Table 7: Command syntax for upgrading IronWare image on the management module

Command syntax	Description
copy tftp flash <TFTP-server-ip-addr> <image-name> **primary | secondary**	Copies the images from the TFTP server to the primary or secondary locations in flash memory.
copy tftp slot1 | slot2 <TFTP-server-ip-addr> <image-name> **primary | secondary**	Copies the images from the TFTP server to a flash card.
copy slot1 | slot2 flash <image-name> **primary | secondary**	Copies the images from a flash card to the primary or secondary locations in flash memory.
copy slot1 | slot2 slot1 | slot2 <image-name> <dest-name>	Copies the images from a flash card in slot 1 or slot 2 to another flash card in slot 1 or slot 2.

For example, to copy the management module's Ironware image from TFTP server 10.10.12.12 to flash memory, enter the following command.

```
BigIron RX# copy tftp flash 10.10.12.12 rmpr02800a.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:

    `BigIron RX# show flash` (if the destination was code flash) `BigIron RX# dir /<path-name>/` (if the destination was slot 1 or slot 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 monitor and boot images on the interface module

Note: 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 on an interface module, 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 slot 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 (For example: `BigIron RX#`):

**Table 8: 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 boot and monitor image from TFTP server 10.10.12.12 to the interface module, enter the following command.

```
BigIron RX# copy tftp lp 10.10.12.12 rlb02800a.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:

```
BigIron RX# 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 slot 2.

2. Copy the new IronWare image from the TFTP server or a flash card in slot 1 or slot 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 (For example: BigIron RX#):

Table 9: Command syntax for upgrading IronWare image on the interface module

Command syntax	Description
copy tftp lp <TFTP-server-ip-addr> <image-name> **primary	secondary all**	Copies the images from the TFTP server to the interface module.
copy tftp lp <TFTP-server-ip-addr> <image-name> **primary	secondary** <chassis-slot-number>	Copies the images from the TFTP server to the interface module in the specified chassis slot.
**copy slot1	slot2 lp** <image-name> **primary	secondary all**	Copies the images from a flash card to the interface module.
**copy slot1	slot2 lp** <image-name> **primary	secondary** <chassis-slot-number>	Copies the images from a flash card to the interface module in the specified chassis slot.

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

```
BigIron RX# copy tftp lp 10.10.12.12 rlp02800a.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 02.8.00a version.

Table 10: MBRIDGE versions required per software version

Software image installed on BigIron RX	Current MBRIDGE image	Version	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 02.5.00f	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)
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)
02.8.00 through 02.8.00a	BigIron RX-16/8/4 (mbridge) BigIron RX-32 (mbridge32)	21 21	MP (Management Module)

Table 11: 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

Software image installed on BigIron RX	FPGA image	Compatible FPGA version
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
02.8.00 through 02.8.00a	SBRIDGE	6

To upgrade the MBRIDGE FPGA image on the BigIron RX management module, 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 slot 2.

3. Copy the MBRIDGE FPGA image from the TFTP server or a flash card in slot 1 or slot 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 (For 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:

   ```
   BigIron RX# show version
   ```

Check for the MBRIDGE image version numbers in the output. For more information on the software images installed on BigIron RX, 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:

  - 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.

  - 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 not entered 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, you must 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 Series 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 02.8.00a to 02.8.00b. It is not available when upgrading from software release 02.7.00 to 02.8.00.

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 Series 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.

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

- After hitless upgrade, the BigIron RX Series 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 started 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
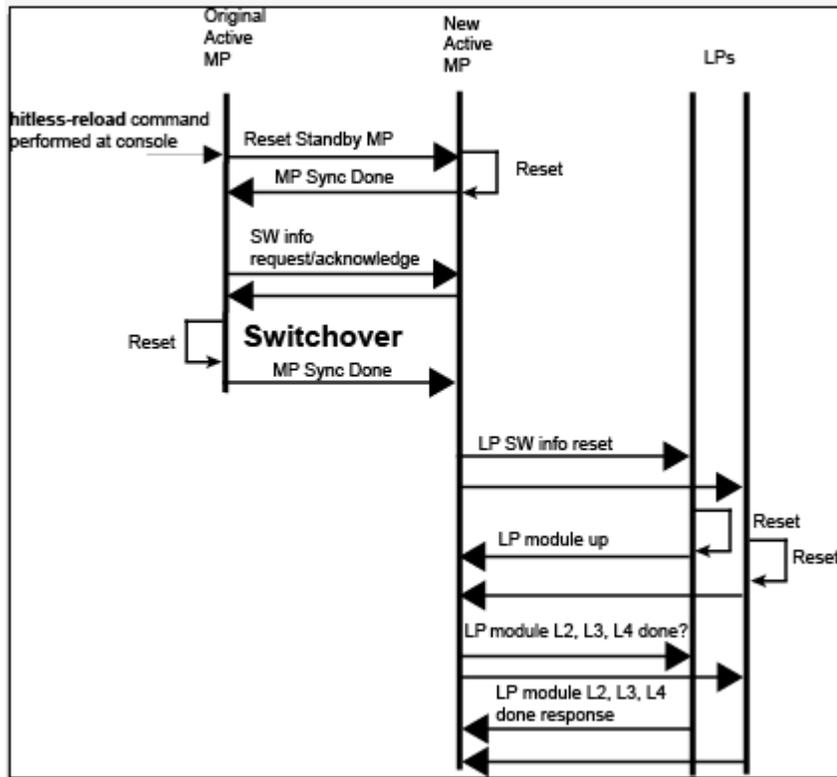
Performing a Hitless Layer 2 OS software upgrade

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 monitor and boot images on the management module 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

If you need to contact Technical Support, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Go to http://www.brocade.com/ethernetproducts to obtain the latest version of the manuals. If you need to report errors in the manuals, send an email to documentation@brocade.com.

Additional resources

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

Table 12: 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 following table, "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 Release 02.8.00a

Defect ID: DEFECT000350761	Technical Severity: Critical
Summary: Under certain VRRP configurations Application Buffers may become depleted.	
Symptom: Under certain VRRP configurations Application Buffers may become depleted causing unexpected reset of the LP.	
Feature: VRRP	Function: VRRPE
Probability: Medium	
Found in Release: RX 02.7.03	Service Request ID: 601157

Defect ID: DEFECT000325041	Technical Severity: Medium
Summary: SNMP PIM interface table query returns inaccurate data.	
Symptom: CLI command "show ip pim int" does not display all interfaces and displays an incorrect mask.	
Feature: SNMP Management	Function: Multicast Mib
Probability: High	
Found in Release: RX 02.7.03	Service Request ID: 264854

Defect ID: DEFECT000355837	Technical Severity: Medium
Summary: Message buffer depletion on management module is possible when duplicate IP address is detected.	
Symptom: In rare conditions, due to buffer depletion all the LPs may reset due to the loss of heartbeat	
Feature: SYSTEM	Function: SNM
Probability: Medium	
Found in Release: RX 02.7.03	Service Request ID: 631847

Defect ID: DEFECT000362014	Technical Severity: Medium
Summary: The CLI command "show memory" may show a negative value for os_malloc count and os_free count, after some time.	
Symptom: Display problem only in the "show memory" values for os_malloc count and os_free count showing negative values.	
Feature: SYSTEM	Function: Flash memory
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID: 646359

Defect ID: DEFECT000352293	Technical Severity: Medium
Summary:	Burst of jumbo frames may cause forwarding to cease on some ports of the 16x10 modules.
Symptom:	With 8Gb/s of ISCI traffic at layer-2 sent through the RX, the traffic was balanced across 2 10G ports on ingress and 2 on egress. These 10G ports were on 16x10 modules.
	For example, ingress ports could be 3/5, 4/5 and egress 3/1 4/1. When one of the ingress ports was disabled, with flow-control enabled, the remaining port would stop forwarding traffic until the disabled port was reenabled.
	However with flow-control removed from the remaining enabled, port and the failover repeated, the port would keep forwarding traffic and accept the aggregate load of around 8Gb/s.
Workaround: Remove flow-control on port.	
Feature: SYSTEM	Function: Buffer Manger
Probability: Medium	
Found in Release: RX 02.7.03	Service Request ID: 614671

Defect ID: DEFECT000358629	Technical Severity: Medium
Summary:	Memory depletion in global pool on standby management module. This happens over a period time as a results of writting configuration to memory ("write memory").
Symptom:	This may occur when trying to use "wr mem" and received the following error
	Write startup-config done.
	Copy STARTUP CONFIG FILE to standby MP, please wait.
	Error: Sync startup config to standby MP failed (RECEIVER OUT OF MEMORY).
Feature: SYSTEM	Function: Buffer Manger
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 637627

Defect ID: DEFECT000359137	Technical Severity: Medium
Summary: Line cards could reset if PIM-SM is enabled.	
Symptom: In some cases unexpected reset may occur on multiple line cards.	
Feature: IPv4 MC-Snooping (VLAN)	Function: IGMP Snooping
Probability: High	
Found in Release: RX 02.8.00	Service Request ID: 636749:

Defect ID: DEFECT000362113	Technical Severity: Low
Summary: Active and standly MP slot numbers are being displayed as 33 and 34 in RX-4, 8, 16	
Symptom: Display issue with the standy and active MP slots.	
Feature: Console	Function: DISPLAY
Probability: High	
Found in Release: RX 02.7.02	Service Request ID:

Defect ID: DEFECT000355173	Technical Severity: Low
Summary: Adding hidden command to disable internal ACLs for BGP and BFD	
Symptom: Adding hidden command to disable internal ACLs for BGP and BFD. This has been reported by US-CERT http://www.kb.cert.org/vuls/id/853246.	
Feature: ACL	Function: IPv4
Probability: Low	
Found in Release: RX 02.8.00	Service Request ID:

Closed defects with code change in Multi-Service IronWare Release 02.8.00

Defect ID: DEFECT000336030	Technical Severity: Critical
Summary: Interface Module unexpectedly reloaded due to IPv6 packet that caused some internal looping when processing	
Feature: IPv6 Forwarding	Function: FIB
Probability: Low	
Found in Release: RX 02.7.00	Service Request ID: 522363

Defect ID: DEFECT000343061	Technical Severity: Critical
Summary: The management module unexpectedly reloaded due to AAA abnormal activity.	
Symptom: The reload caused a switchover with redundant management modules.	
Feature: AAA	Function: AAA Engine
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID: 577115

Defect ID: DEFECT000338374	Technical Severity: Critical
Summary: Secondary next-hop in PBR is not taking effect when static route is also configured.	
Symptom: Cannot use secondary PBR when primary PBR is down.	
Feature: IPv4 Forwarding	Function: PBR
Probability: Medium	
Found in Release: RX 02.7.03	Service Request ID: 505151

Defect ID: DEFECT000341616	Technical Severity: Critical
Summary: Multiple Interface Modules unexpectedly reloaded after issuing a "show ip route x.x.x.x debug" command.	
Feature: CLI Infrastructure	Function: Parser Engine
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID: 565463

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

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.	
Feature: L2 Protocol	Function: VSRP1
Probability: Medium	
Found in Release: RX 02.4.00	Service Request ID: 178709

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	
Feature: DNS	Function: PROTOCOL
Probability: High	
Found in Release: RX 02.7.00	Service Request ID: 215029

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.	
Feature: IPv4 MC-Snooping (VLAN)	Function: IGMP Snooping
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID:

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.	
Feature: OSPF	Function: Redistribution
Probability: High	
Found in Release: RX 02.7.00	Service Request ID: 260272

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.	
Feature: CLI Infrastructure	Function: Parser Engine
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID: 265696

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.	
Feature: OSPF	Function: PROTOCOL
Probability: High	
Found in Release: RX 02.7.02	Service Request ID: 248796

Defect ID: DEFECT000340501	**Technical Severity**: High
Summary: Issuing the OSPF command 'no ip ospf network point-to-point' on VE interface may cause an unexpected reset.	
Symptom: After changing the OSPF parameter 'no ip ospf network point-to-point' on a VE (VE71).the router reset immediately.	
Feature: OSPF	**Function**: CONFIGURATION
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 552751

Defect ID: DEFECT000300236	**Technical Severity**: Medium
Summary: RX only sends SNMPv1 traps, and there is no way to generate traps in SNMPv2 or SNMPv3.	
Symptom: Unable to generate traps in SNMPv2 or SNMPv3.	
Feature: SNMP Management	**Function**: Trap/Notification
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 249438

Defect ID: DEFECT000336870	**Technical Severity**: Medium
Summary: New power supplies are showing up as AC power supply, when "show chassis" command is executed, even though it is a DC power supply.	
Symptom: DC power supplies are showing up as AC power supplies, when "show chassis" command is executed. *** BigIron RX-16 CHASSIS *** ---POWERS --- Power 1 (32009000 - DC 1200W): Installed (OK) Power 2 (32009000 - DC 1200W): Installed (OK) Power 3 (32009000 - DC 1200W): Installed (OK) Power 4: Installed (Failed) Power 5 (32009000 - DC 1200W): Installed (OK) Power 6 (32009000 - DC 1200W): Installed (OK) Power 7 (32050 - AC 1200W): Installed (OK) Power 8 (32050 - AC 1200W): Installed (OK) Total power budget for chassis = 8400W	
Feature: SYSTEM	**Function**: POWER SUPPLY
Probability: High	
Found in Release: RX 02.7.02	**Service Request ID**: 522907

Defect ID: DEFECT000343072	**Technical Severity**: Medium
Summary: BGP session resets after generating invalid MBGP update with large attribute size.	
Feature: BGP	**Function**: BGPv4
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 550649

Defect ID: DEFECT000340184	Technical Severity: Medium
Summary: SNMP unable to get area ID from ospfAreaId table when backbone area 0 or 0.0.0.0 is not configured	
Symptom: Unable to get the OSPF area ID from MIB. This works correctly when area 0 is present.	
Feature: SNMP Management	Function: Routing Mib
Probability: High	
Found in Release: RX 02.5.00	Service Request ID: 536863

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.	
Feature: IPv4 Forwarding	Function: ARP
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 265832

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.	
Feature: CLI Infrastructure	Function: Page Mode Display
Probability: Low	
Found in Release: RX 02.7.02	Service Request ID: 241827

Defect ID: DEFECT000336038	Technical Severity: Medium
Summary: Static Group to RP Mapping not in sync between the MP and LP.	
Symptom: Group to RP Mapping not in sync between the MP and LP.	
Workaround: Use Numbered ACL , instead of using the named ACL.	
Feature: IPv4-MC PIM-SM Routing	Function: Static RP
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 535449

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.	
Feature: IPv4-MC PIM-SM Routing	Function: PROTOCOL
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 267599

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

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.	
Feature: IPv4 Forwarding	Function: Next Hop Table
Probability: High	
Found in Release: RX 02.7.02	Service Request ID: 265521

Defect ID: DEFECT000325133	Technical Severity: Medium
Summary: Simultaneous use of IPv6 and IPv4 ACLs is not possible.	
Feature: ACL	Function: IPV6
Probability: Medium	
Found in Release: RX 02.7.03	Service Request ID:

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.	
Feature: OSPF	Function: show commands
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 262838

Defect ID: DEFECT000280574	Technical Severity: Medium
Summary: L2 ACL-based mirroring does not work correctly.	
Feature: Mirroring	Function: ACL Based
Probability: High	
Found in Release: RX 02.7.03	Service Request ID: 241515

Defect ID: DEFECT000315502	Technical Severity: Medium
Summary: L2 registration process changed between release 2.5.00x and 2.7.02 without having backward compatibility support in new code.	
Feature: IPv4-MC PIM-SM Routing	Function: PROTOCOL
Probability: Medium	
Found in Release: RX 02.7.02	Service Request ID: 249362

Defect ID: DEFECT000299437	Technical Severity: Medium
Summary: MP CPU may experience some memory leakage IN SNMP while polling snAgentTempSensorDescr	
Symptom: The memory leak is happening in the GET and GET-NEXT operation for snAgentTempSensorDescr of snAgentTempTable. Because of the unnecessary allocation of memory.	
Feature: SNMP Management	Function: Engine
Probability: High	
Found in Release: RX 02.7.02	Service Request ID: 245942

Defect ID: DEFECT000287890	Technical Severity: Medium
Summary: BGP "allowas-in" does not work correctly with confederation configuration.	
Symptom: BGP Routes received from peer with local AS (in as-path) are dropped even though "allowas-in" is used for that particular peer. This issue observed only when confederation is configured, wIthout confederation it works as expected.	
Feature: BGP	**Function**: BGPv4
Probability: High	
Found in Release: RX 02.7.00	**Service Request ID**:
Where Else Fixed: PATCH: RX 02.7.02 f	

Defect ID: DEFECT000281680	Technical Severity: Medium
Summary: SNMP GET on The SNMPEngineTime does not return the correct system uptime.	
Feature: SNMP Management	**Function**: Trap/Notification
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 242084
Where Else Fixed: PATCH: RX 02.7.02 f	

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

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.	
Feature: IPv4 MC-Snooping (VLAN)	**Function**: IGMPv3 Snooping
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 240868
Where Else Fixed: PATCH: RX 02.7.02 f	

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 wtih IP address of the interface where they come out.	
Workaround: Downgrade to 2.6.00 tree	
Feature: SYSLOG	**Function**: System Integration
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 237819

Defect ID: DEFECT000274156	Technical Severity: Medium
Summary: Executing command "show interface slot 0" may cause a system reset.	
Symptom: System may reload.	
Feature: CLI Infrastructure	**Function**: Parser Engine
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 238294
Where Else Fixed: PATCH: RX 02.7.02 e	

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.	
Feature: IPv4-MC PIM-SM Routing	**Function**: PROTOCOL
Probability: Low	
Found in Release: RX 02.6.00	**Service Request ID**: 224751
Where Else Fixed: PATCH: RX 02.7.02 e	

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.	
Feature: SYSTEM	**Function**: Tiger HAL
Probability: Medium	
Found in Release: RX 02.6.00	**Service Request ID**: 231524

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

Defect ID: DEFECT000283672	Technical Severity: Medium
Summary: BGP speaker does not advertise update to origin AS	
Symptom: The ability to advertise eBGP update received from a router in AS <N> to a different router in AS <N> is supported on the MLX but is currently not available on the RX.	
Feature: BGP	**Function**: BGPv4
Probability: High	
Found in Release: RX 02.7.02	**Service Request ID**: 243183
Where Else Fixed: PATCH: RX 02.7.02 f	

Defect ID: DEFECT000350901	Technical Severity: Medium
Summary: IPv6 SNMP-client not displayed in running configuration.	
Symptom: Unable to add "snmp-client ipv6 2606:8200::ffff" to the configuration. When configuring the clause, the system seemed to take the command without any warning, but running configuration did not appear to save it.	
Feature: SNMP Management	**Function**: CLI
Probability: High	
Found in Release: RX 02.7.02	**Service Request ID**: 613853

Defect ID: DEFECT000279953	Technical Severity: Medium
Summary: STP BPDUs may be dropped across the Q-in-Q link	
Feature: L2 Protocol	**Function**: STP
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 238581
Where Else Fixed: PATCH: RX 02.7.02 e	

Defect ID: DEFECT000343291	Technical Severity: Medium
Summary: gig-default neg-off previously configured as gig-default auto-full does not activate link	
Symptom: A "gig-default auto-full" configured port does not get to link up state if the other end of the link has "auto negotiation" disabled on the port. To get the link up, must remove "gig-default auto-full" once and then add it again.	
Feature: SYSTEM	**Function**: Auto-negotiation
Probability: Medium	
Found in Release: RX 02.7.02	**Service Request ID**: 555549