Release Notes for Cisco IOS XR Software Release 3.2.6

August 21, 2006

Cisco IOS XR Software Release 3.2.6

Text Part Number OL-11380-02

Note See the "Important Notes" section on page 12 for important information on Cisco IOS XR Software Release 3.2.6.

Note You can find the most current Cisco IOS XR software documentation on the World Wide Web at http://www.cisco.com/en/US/products/ps5845/tsd_products_support_series_home.html. These electronic documents might contain updates and modifications. See the "Obtaining Documentation" section on page 25 for more information on obtaining Cisco documentation.

These release notes describe the features provided in Cisco IOS XR Software Release 3.2.6 and are updated as needed.

For a list of software caveats that apply to Cisco IOS XR Software Release 3.2.6, see the "Caveats" section on page 14. The caveats are updated for every release and are located on the World Wide Web at www.cisco.com.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected, at http://www.cisco.com/public/support/tac/fn_index.html.

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

Contents

These release notes contain the following sections:

Introduction

Cisco IOS XR software is a distributed operating system designed for continuous system operation combined with service flexibility and high performance.

Cisco IOS XR software provides the following features and benefits:

- *IP and Routing*—Supports a wide range of IPv4 and IPv6 services, and routing protocols, such as Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), IP Multicast, Routing Policy Language (RPL), and Hot Standby Router Protocol (HSRP)/Virtual Router Redundancy Protocol features (VRRP).
- *Bidirectional forwarding detection (BFD)*—Provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. The fast detection of failures provides immediate reaction to failure in the event of a failed link or neighbor. OSPF, ISIS, BGP, and MPLS-TE FRR use BFD to detect failures (Cisco CRS-1 routers only).
- *MPLS*—Supports Multiprotocol Label Switching (MPLS) protocols such as Traffic Engineering (TE), Resource Reservation Protocol (RSVP), and Label Distribution Protocol (LDP).
- *Multicast*—Provides comprehensive IP Multicast software including Source Specific Multicast (SSM). The Cisco CRS-1 router supports Bidirectional Protocol Independent Multicast (BIDIR-PIM).
- *Quality of service (QoS)*—Supports rich QoS mechanisms including policing, marking, queuing, dropping, and shaping. Additionally, the operating systems support Modular QoS CLI (MQC). MQC is used to configure various QoS features on various Cisco platforms.

- *Manageability*—Provides industry-standard management interfaces including modular command-line interface (CLI), Simple Network Management Protocol (SNMP), and native Extensible Markup Language (XML) interfaces.
- *Security*—Provides comprehensive network security features including access control lists (ACLs), routing authentications, AAA/TACACS+, Secure Shell (SSH), SNMPv3, and leading Routing Policy Language (RPL) support. Control-plane protections integrated into line card ASICs include Generalized TTL Security Mechanism (GTSM), RFC 3682, and dynamic control plane protection.
- *Craft Works Interface (CWI)*—A client-side application used to configure and manage Cisco routers. The management and configuration features include fault, configuration, security, and inventory, with an emphasis on speed and efficiency. The CWI provides a context-sensitive graphical representation of the objects in a Cisco router, simplifying the process of configuring and managing the router. The CWI allows you to log in to multiple routers and perform management tasks.
- *Availability*—Supports rich availability features such as fault containment, fault tolerance, fast switchover, link aggregation, and nonstop forwarding (NSF).
- *In Service Software Upgrade (ISSU)*—Supports a modular-packaging-based release model to minimize the impact of upgrades and supports ISSU with NSF, where possible.

See the "New and Changed Information for Release 3.2.6" section on page 12 for a detailed list of new features by platform for Cisco IOS XR Software Release 3.2.6.

System Requirements

The Cisco IOS XR Software Release 3.2.6 is supported on the following platforms:

Cisco CRS-1 Router

This section describes the system requirements for Cisco IOS XR software Release 3.2.6 supported on Cisco CRS-1 routers and includes the following information:

Feature Set Table for the Cisco CRS-1 Router

Cisco IOS XR software is packaged in feature sets (also called software images). Each feature set contains a specific set of Cisco IOS XR Software Release 3.2.6 features. Table 1 and Table 2 list the Cisco IOS XR software feature set matrix and associated filenames that are available for the Cisco IOS XR Software Release 3.2.6 that is supported on the Cisco CRS-1 router.

Table 1 Cisco CRS-1 Supported Feature Sets (Cisco IOS XR Software Release 3.2.6 PIE Files)

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR Unicast Routing Core Bundle	comp-hfr-mini.pie-3.2.6	Contains the required core packages, including OS, Admin, Base, Forwarding, Modular Services Card, and Routing packages.
Optional Individual Packages[1]		
Cisco IOS XR Manageability Package	hfr-mgbl-p.pie-3.2.6	CORBA agent, XML Parser, HTTP server, SNMP Agent, and Alarm correlation.
Cisco IOS XR MPLS Package	hfr-mpls-p.pie-3.2.6	MPLS-TE, LDP, MPLS-TE Link Management, MPLS Forwarding, Optical Link Management, OUNI, and RSVP.
Cisco IOS XR Multicast Package	hfr-mcast-p.pie-3.2.6	Multicast Routing Protocols (PIM, MSDP, IGMP, Auto-RP), Tools (SAP, MTrace), Infrastructure (MRIB, MURIB, MFWD), and BIDIR.
Cisco IOS XR Security Package	hfr-k9sec-p.pie-3.2.6	Support for encryption, decryption, IPSec, SSH, SSL, and PKI.

1. Packages are installed individually.

Table 2 Cisco CRS-1 Supported Feature Sets (Cisco IOS XR Software Release 3.2.6 TAR Files)

Feature Set	Filename	Description
Cisco IOS XR IP/MPLS Core Software	CRS-1-iosxr-3.2.6.tar	Tar file containing: • Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS XR MPLS Package • Cisco IOS XR Multicast Package
Cisco IOS XR IP/MPLS Core Software 3DES	CRS-1-iosxr-k9-3.2.6.tar	Tar file containing: • Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS XR MPLS Package • Cisco IOS XR Multicast Package • Cisco IOS XR Security Package

Memory Requirements for the Cisco CRS-1 Router

The minimum memory requirements for a Cisco CRS-1 router that is running Cisco IOS XR Software Release 3.2.6 are:

- 2-GB memory on the route processors (RPs)
- 1-GB memory on the modular services cards (MSCs)

Hardware Supported for the Cisco CRS-1 Router

Cisco IOS XR Software Release 3.2.6 supports Cisco CRS-1 routers. All hardware features are supported on Cisco IOS XR software, subject to the memory requirements specified in the "Memory Requirements for the Cisco CRS-1 Router" section on page 5.

Table 3 lists the hardware components supported on the Cisco CRS-1 router and the minimum versions required. See the "Determining the Software Version for the Cisco CRS-1 Router" section on page 7.

Table 3 Cisco CRS-1 Supported Hardware and Minimum Software Requirements

Component	Part Number	Minimum Software Version Required
Cisco CRS-1 Series 16-Slot Line Card Chassis		
Cisco CRS-1 16-Slot Line Card Chassis	CRS-16-LCC	3.2.x
Cisco CRS-1 Fan Tray for 16-Slot LCC	CRS-16-LCC-FAN-TR	3.2.x
Cisco CRS-1 16-Slot Fabric Card/Single	CRS-16-FC/S	3.2.x
Cisco CRS-1 Fan Controller for 16-Slot Line Card Chassis	CRS-16-LCC-FAN-CT	3.2.x
Cisco CRS-1 16-Slot Route Processor	CRS-16-RP	3.2.x
Cisco CRS-1 Memory Module 2 GB	CRS-MEM-2G	3.2.x
Cisco CRS-1 PCMCIA Flash Disk 1 GB	CRS-FLASH-DISK-1G	3.2.x
Cisco CRS-1 Modular Services Card	CRS-MSC	3.2.x
Cisco CRS-1 LCC Front AC Power Panel	CRS-16-ACGRILLE	3.2.x
Cisco CRS-1 LCC Front DC Power Panel	CRS-16-DCGRILLE	3.2.x
Cisco CRS-1 16-Slot Alarm Board	CRS-16-ALARM	3.2.x
Cisco CRS-1 AC Delta Power Shelf for 16-Slot LCC	CRS-16-LCC-PS-ACD	3.2.x
Cisco CRS-1 AC Wye Power Shelf for 16-Slot LCC	CRS-16-LCC-PS-ACW	3.2.x
Cisco CRS-1 DC Power Shelf for 16-Slot LCC	CRS-1-LCC-PS-DC	3.2.x
Cisco CRS-1 4xOC-192/STM64 POS/DPT Interface Module/VS	4OC192-POS/DPT-VS	3.2.x
Cisco CRS-1 4xOC-192/STM64 POS/DPT Interface Module/SR	4OC192-POS/DPT-SR	3.2.x
Cisco CRS-1 4xOC-192/STM64 POS/DPT Interface Module/IR	4OC192-POS/DPT-IR	3.2.x
Cisco CRS-1 4xOC-192/STM64 POS/DPT Interface Module/LR	4OC192-POS/DPT-LR	3.2.x
Cisco CRS-1 16xOC-48/STM16 POS/DPT Interface Module	16OC48-POS/DPT	3.2.x
Cisco CRS-1 2.5 G SFP LR Optic	POM-OC48-LR2-LC-C	3.2.x
Cisco CRS-1 2.5 G SFP SR Optic	POM-OC48-SR-LC-C	3.2.x
Cisco CRS-1 Line Card Chassis Front Doors	CRS-16-LCC-DRS-F	3.2.x

Table 3 Cisco CRS-1 Supported Hardware and Minimum Software Requirements (continued)

Component	Part Number	Minimum Software Version Required
Cisco CRS-1 Line Card Chassis Front Cable Mgmt	CRS-16-LCC-FRNT	3.2.x
Cisco CRS-1 LCC Expanded Front Cable Mgmt	CRS-16-LCC-FRNT-E	3.2.x
Cisco CRS-1 Line Card Chassis Rear Cable Mgmt	CRS-16-LCC-BCK-CM	3.2.x
Cisco CRS-1 Line Card Chassis Rear Doors	CRS-16-LCC-DRS-R	3.2.x
Cisco CRS-1 Lift for LCC 16 and FCC	CRS-16-LIFT	3.2.x
Cisco CRS-1 Series 8-Slot Line Card Chassis		
Cisco CRS-1 8-Slot Line Card Chassis	CRS-8-LCC	3.2.x
Cisco CRS-1 Fan Tray for 8-Slot Line Card Chassis	CRS-8-LCC-FAN-TR	3.2.x
Cisco CRS-1 Line Card Chassis Filter Pack	CRS-8-LCC-FILTER	3.2.x
Cisco CRS-1 AC Pwr Rectifier for 8-Slot LCC	CRS-8-AC-RECT	3.2.x
Cisco CRS-1 DC Power Entry Module for 8-Slot LCC	CRS-8-DC-PEM	3.2.x
Cisco CRS-1 AC & DC Power Module Filter for 8-Slot LCC	CRS-8-PWR-FILTER	3.2.x
Cisco CRS-1 AC Delta PDU for CRS-8 LCC	CRS-8-LCC-PDU-ACD	3.2.x
Cisco CRS-1 AC Wye PDU for CRS-8 LCC	CRS-8-LCC-PDU-ACW	3.2.x
Cisco CRS-1 DC PDU for CRS-8 LCC	CRS-8-LCC-PDU-DC	3.2.x
Cisco CRS-1 8-Slot Fabric Card/Single	CRS-8-FC/S	3.2.x
Cisco CRS-1 8-Slot Fabric Card Blank	CRS-8-FC-BLANK	3.2.x
Cisco CRS-1 8-Slot Fabric Handle	CRS-8-FC-HANDLE	3.2.x
Cisco CRS-1 8-Slot Route Processor	CRS-8-RP	3.2.x
Cisco CRS-1 8-Slot Route Processor Blank	CRS-8-RP-BLANK	3.2.x
Cisco CRS-1 8-Slot Route Processor Handle	CRS-8-RP-HANDLE	3.2.x
Cisco CRS-1 8x10 GbE Interface Module/LR	8-10GBE	3.2.x
10GBASE-LR XENPAK Module for CRS-1	CRS-XENPAK10GB-LR	3.2.x
10GBASE-DWDM XENPAK	CRS-1 CRS-XENPAK10GB-DWDM	3.2.2
Cisco CRS-1 4xOC-192/STM64 POS/DPT Interface Module/LR	4OC192-POS/DPT-LR	3.2.x
Cisco CRS-1 1xOC-768/STM256 POS Interface Module/SR	1OC768-POS-SR	3.2.x
Cisco CRS-1 8-Slot Install Kit	CRS-8-INSTALL-KT	N/A
Cisco CRS-1 8-Slot Fork Lift Tube	CRS-8-LIFT-TUBE	N/A
Cisco CRS-1 8-Slot Front Badge Panel	CRS-8-BDG-PANEL	N/A
Cisco CRS-1 8-Slot Front Inlet Grill	CRS-8-FRNT-GRILL	N/A
Cisco CRS-1 8-Slot Horizontal Install Rails	CRS-8-HRZ-RAILS	N/A
Cisco Carrier 1 Series SPA Interface Processor 40G	CRS1-SIP-800	3.2.x
Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics	SPA-OC192POS-XFP	3.2.x

Table 3 Cisco CRS-1 Supported Hardware and Minimum Software Requirements (continued)

Component	Part Number	Minimum Software Version Required
Cisco 8-Port Gigabit Ethernet Shared Port Adapter	SPA-8X1GE	3.2.x
Cisco 4-Port OC-3 Shared Port Adapter	SPA-4XOC3-POS	3.2.x

Software Compatibility for the Cisco CRS-1 Router

Cisco IOS XR Software Release 3.2.6 is compatible with the Cisco CRS-1 systems:

- Cisco CRS-1 8-Slot Line Card Chassis
- Cisco CRS-1 16-Slot Line Card Chassis

Determining the Software Version for the Cisco CRS-1 Router

To determine the version of Cisco IOS XR software running on your router, log in to the router and enter the **show version** command:

Step 1 Establish a Telnet session with the router.

Step 2 Enter the **show version** command:

```
Cisco IOS XR Software, Version 3.2.6[00]
Copyright (c) 2006 by cisco Systems, Inc.
ROM: System Bootstrap, Version 1.40(20060413:002654) [CRS-1 ROMMON],
MPLS-MR-2 uptime is 1 day, 16 hours, 59 minutes
System image file is "disk0:hfr-os-mbi-3.2.6/mbihfr-rp.vm"
cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revision 1.1
20 Packet over SONET network interface(s)
20 SONET/SDH Port controller(s)
8 TenGigabitEthernet/IEEE 802.3 interface(s)
1 Ethernet/IEEE 802.3 interface(s)
8 GigabitEthernet/IEEE 802.3 interface(s)
2043k bytes of non-volatile configuration memory.
38079M bytes of hard disk.
1000592k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).

hfr-admin, V 3.2.6[00], Cisco Systems, at disk0:hfr-admin-3.2.6
Built on Tue Aug 8 14:06:26 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-base, V 3.2.6[00], Cisco Systems, at disk0:hfr-base-3.2.6
Built on Tue Aug 8 13:54:28 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-os-mbi, V 3.2.6[00], Cisco Systems, at disk0:hfr-os-mbi-3.2.6
Built on Tue Aug 8 13:10:15 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-mcast, V 3.2.6[00], Cisco Systems, at disk0:hfr-mcast-3.2.6
Built on Tue Aug 8 14:37:43 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-mpls, V 3.2.6[00], Cisco Systems, at disk0:hfr-mpls-3.2.6
Built on Tue Aug 8 14:30:38 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8
```

```
hfr-lc, V 3.2.6[00], Cisco Systems, at disk0:hfr-lc-3.2.6
Built on Tue Aug 8 14:23:55 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-fwdg, V 3.2.6[00], Cisco Systems, at disk0:hfr-fwdg-3.2.6
Built on Tue Aug 8 14:12:04 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-admin, V 3.2.6[00], Cisco Systems, at disk0:hfr-admin-3.2.6
Built on Tue Aug 8 14:06:26 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-base, V 3.2.6[00], Cisco Systems, at disk0:hfr-base-3.2.6
Built on Tue Aug 8 13:54:28 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-os-mbi, V 3.2.6[00], Cisco Systems, at disk0:hfr-os-mbi-3.2.6
Built on Tue Aug 8 13:10:15 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-admin, V 3.2.6[00], Cisco Systems, at disk0:hfr-admin-3.2.6
Built on Tue Aug 8 14:06:26 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-base, V 3.2.6[00], Cisco Systems, at disk0:hfr-base-3.2.6
Built on Tue Aug 8 13:54:28 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-os-mbi, V 3.2.6[00], Cisco Systems, at disk0:hfr-os-mbi-3.2.6
Built on Tue Aug 8 13:10:15 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

hfr-mcast, V 3.2.6[00], Cisco Systems, at disk0:hfr-mcast-3.2.6
Built on Tue Aug 8 14:37:43 PDT 2006
By ccms-view1 in /vws/srz/dwperon/production/3.2.6.00/hfr/workspace for c2.95.3-p8

< truncated remainder of lengthy output >
```

Other Firmware Code for the Cisco CRS-1 Router

The following firmware code is supported by the Cisco CRS-1 router:

- The minimum ROMMON version required for this release is 1.38.

Note Be sure to upgrade the ROMMONs to version 1.38 *before* attempting the upgrade. The following URL points to procedures for a Cisco CRS-1 router:

http://www.cisco.com/cgi-bin/tablebuild.pl/crs1rommon

- The minimum CPUCTRL version required for this release is 2.07.
- For detailed information on ROMMON, refer to *Cisco IOS XR Getting Started Guide*.

Cisco XR 12000 Series Router

This section describes the system requirements for Cisco IOS XR Software Release 3.2.6 supported on the Cisco XR 12000 Series Router and includes the following information:

Note Release 3.2.6 contains software refinements for the Cisco IOS XR router only. Therefore, for the Cisco XR 12000 Series Router, Release 3.2.3 features and compatibility information are presented in these Release 3.2.6 release notes.

Feature Set Table for the Cisco XR 12000 Series Router

The Cisco IOS XR software is packaged in feature sets (also called software images). Each feature set contains a specific set of Cisco IOS XR Software Release 3.2.3 features. Table 4 and Table 5 list the Cisco IOS XR software feature set matrix and associated filenames available for Cisco IOS XR software Release 3.2.3 supported on the Cisco XR 12000 Series Router.

Table 4 Cisco XR 12000 Series Router Supported Feature Sets (Cisco IOS XR Software Release 3.2.3 PIE Files)

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR Unicast Routing Core Bundle	c12k-mini.vm-3.2.3	Contains the required core packages including, OS, Admin, Base, Forwarding, Line Cards, and Routing packages.
Optional Individual Packages[1]		
Cisco IOS XR Manageability Package	c12k-mgbl.pie-3.2.3	CORBA agent, XML Parser, HTTP server, SNMP agent, and Alarm correlation.
Cisco IOS XR MPLS Package	c12k-mpls.pie-3.2.3	MPLS-TE, LDP, MPLS-TE Link Management, MPLS Forwarding and RSVP.
Cisco IOS XR Multicast Package	c12k-mcast.pie-3.2.3	Multicast Routing Protocols (PIM, MSDP, IGMP, Auto-RP), Tools (SAP, MTrace), and Infrastructure (MRIB, MURIB, MFWD).
Cisco IOS XR Security Package	c12k-k9sec.pie-3.2.3	Support for Encryption, Decryption, IPSec, SSH, SSL, and PKI.
Cisco IOS XR Standby RP Boot Image	mbiprp-rp.vm-3.2.3	Support for booting the standby RP on a Cisco XR 12000 Series Router (PRP).

1. Packages are installed individually.

Table 5 Cisco XR 12000 Series Router Supported Feature Sets (Cisco IOS XR Software Release 3.2.3 TAR Files)

Feature Set	Filename	Description
Cisco IOS XR IP/MPLS Core Software	C12000-iosxr-3.2.3.tar	Tar file containing: • Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS XR MPLS Package • Cisco IOS XR Multicast Package
Cisco IOS XR IP/MPLS Core Software 3DES	C12000-iosxr-k9-3.2.3.tar	Tar file containing: • Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS XR MPLS Package • Cisco IOS XR Multicast Package • Cisco IOS XR Security Package

Memory Requirements for the Cisco XR 12000 Series Router

The minimum memory requirements for Cisco XR 12000 Series Router routers running Cisco IOS XR Software Release 3.2.3 are:

- 1 GB of route memory on Performance Route Processor 1 (PRP-1) and Performance Route Processor 2 (PRP-2)
- 512-MB ATA flash storage on PRP-1 and PRP-2 (1-GB ATA flash is recommended)
- 512-MB line-card packet and route memory on all line cards installed in the system

Hardware Supported for the Cisco XR 12000 Series Router

Cisco IOS XR Software Release 3.2.3 supports the Cisco XR 12000 Series Router. All hardware features are supported on Cisco IOS XR software, subject to the memory requirements specified in the "Memory Requirements for the Cisco XR 12000 Series Router" section on page 10.

Table 6 lists the hardware components supported on the Cisco XR 12000 Series Router and the minimum software versions required.

Table 6 Cisco XR 12000 Series Router Supported Hardware and Minimum Software Requirements

Component	Part Number	Minimum Software Version Required
Cisco XR 12000 Series Router 12404/80 Chassis	GSR4/80-xx	3.2.x
Cisco XR 12000 Series Router 12406/120 Chassis	GSR6/120-AC	3.2.x
Cisco XR 12000 Series Router 12410/200 Chassis	GSR10/200-xx	3.2.x
Cisco XR 12000 Series Router 12416/320 Chassis	GSR16/320-xx	3.2.x
Cisco XR 12000 Series Router Performance Route Processor 1 (PRP-2 is strongly recommended)	PRP-1	3.2.x
Cisco XR 12000 Series Router Performance Route Processor 2	PRP-2	3.2.x

Table 6 Cisco XR 12000 Series Router Supported Hardware and Minimum Software Requirements (continued)

Component	Part Number	Minimum Software Version Required
Cisco XR 12000 Series Router 40 GB Hard Drive Option	HD-PRP2-40G	3.2.x
Cisco XR 12000 Series Router 4xOC12c/STM4c POS Intermediate Reach Single-Mode optics	4OC12X/POS-I-SC-B	3.2.x
Cisco XR 12000 Series Router 4xOC12c/STM4c POS Short Reach Multi-Mode optics	4OC12X/POS-M-SC-B	3.2.x
Cisco XR 12000 Series Router 16xOC3c/STM1c POS Short Reach Multi-Mode optics	16OC3X/POS-M-MJ-B	3.2.x
Cisco XR 12000 Series Router 16xOC3c/STM1c POS Intermediate Reach Single-Mode optics	16OC3X/POS-I-LC-B	3.2.x
Cisco XR 12000 Series Router 8xOC3c/STM1c POS Short Reach Multi-Mode optics	8OC3X/POS-MM-MJ-B	3.2.x
Cisco XR 12000 Series Router 8xOC3c/STM1c POS Intermediate Reach Single-Mode optics	8OC3X/POS-IR-LC-B	3.2.x
Cisco XR 12000 Series Router 4xOC3c/STM1c POS Short Reach Multi-Mode optics	4OC3X/POS-MM-MJ-B	3.2.x
Cisco XR 12000 Series Router 4xOC3c/STM1c POS Intermediate Reach Single-Mode optics	4OC3X/POS-IR-LC-B	3.2.x
Cisco XR 12000 Series Router 4xOC3c/STM1c POS Long Reach Single-Mode optics	4OC3X/POS-LR-LC-B	3.2.x
Cisco XR 12000 Series Router 1xOC48c/STM16c POS Short Reach Single-Mode optics	OC48X/POS-SR-SC	3.2.x
Cisco XR 12000 Series Router 1xOC48c/STM16c POS Long Reach Single-Mode optics	OC48X/POS-LR-SC	3.2.x
Cisco XR 12000 Series Router 4xGE with SFP optics	4GE-SFP-LC	3.2.x
Cisco XR 12000 Series Router SPA Interface Processor 10G	12000-SIP-600	3.2.x
Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with VSR Optics	SPA-OC192-POS-VSR	3.2.x
Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with LR Optics	SPA-OC192-POS-LR	3.2.x
Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics	SPA-OC192-POS-XFP	3.2.x
Cisco 5-Port Gigabit Ethernet Shared Port Adapter with SFPoptics	SPA-5X1GE	3.2.x
Cisco 10-Port Gigabit Ethernet Shared Port Adapter with SFPoptics	SPA-10X1GE	3.2.x
Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter with XFPoptics	SPA-1XTENGE-XFP	3.2.x

Software Compatibility for the Cisco XR 12000 Series Router

Cisco IOS XR software Release 3.2.3 is compatible with the Cisco XR 12000 Series Router systems:

- Cisco XR 12416 Router
- Cisco XR 12012 Router

- Cisco XR 12410 Router
- Cisco XR 12008 Router
- Cisco XR 12406 Router
- Cisco XR 12404 Router

Other Firmware Code for the Cisco XR 12000 Series Router

The following firmware code is supported by the Cisco XR 12000 Series Router:

- The minimum ROMMON version required for this release is 1.15. For more information on the minimum ROMMON version required for this release, ROMMON upgrade procedures, and flashdisk information, see the *Upgrading from Cisco IOS to Cisco IOS XR Software on the Cisco 12000 Series Router* document.
- The flashdisk Cisco part numbers are: MEM-12KRP-FD512M (=) and MEM-12KRP-FD1G(=)

New and Changed Information for Release 3.2.6

The following sections contain information on new features in Cisco IOS XR Software Release 3.2.6:

- New Software Features in Cisco IOS XR Software Release 3.2.6, page 12
- Changed Software Features in Cisco IOS XR Software Release 3.2.6, page 12

New Software Features in Cisco IOS XR Software Release 3.2.6

No new software features exist in Cisco IOS XR Software Release 3.2.6.

Changed Software Features in Cisco IOS XR Software Release 3.2.6

No changed software features exist in Cisco IOS XR Software Release 3.2.6.

Important Notes

In certain countries, use of these products might be prohibited and subject to laws, regulations, or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customers must comply with all such applicable laws in the countries in which they intend to use the products.

When upgrading a Cisco XR 12000 Series Router from Cisco IOS to Cisco IOS XR software, use the upgrade instructions we provide to minimize traffic impact. For instructions, see *Upgrading from Cisco IOS to Cisco IOS XR Software on the Cisco 12000 Series Router*, Release 3.2 for procedures.

Follow the instructions we provide for card removal and replacement (fan controller, fabric cards, line cards, RP, and so on) to avoid impacting traffic. See *Cisco IOS XR Getting Started Guide* for procedures.

If you intend to test beyond the combined maximum configuration that we test and publish, contact your Cisco representative to discuss how to engineer a large-scale configuration maximum for your testing.

A Cisco SIP-600 line card (LC) draws more power than previous LCs. If the configuration of power entry modules (PEMs) and other cards brings the power needs close to capacity, sufficient power might not be available when you insert a new card or remove a PEM. The **show environment power-supply table** command can help you plan the system power budget. Before inserting any new card or removing a PEM, use the **show environment power-supply table** command, as in the following example:

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# show env power-supply table

48V Current
R/S/I Module (V) (A)
0/24/* PEM1 46 12
PEM2 47 10
0/25/* PEM1 47 12
PEM2 47 10
Total Power Supplies: 4800W
Redundant Power Supplies: 2400W
Worst Case Power Used: 1559W
Current Power Used: 1022W
Current Redundant Power Available: 1378W
Current Total Power Available: 3778W
Worst Case Redundant Power Available: 841W
Worst Case Total Power Available: 3241W
PID Description Watts
--- ----------- -----
GRP-B Route Processor 38
PRP-1 Cisco 12000 Series Performance Route Processor 60
LC-4OC-3-POS-SM 4 Port Packet Over SONET OC-3c/STM-1 80
4OC3X/POS-MM-MJ-B 4 port ISE OC3 90
8OC3/POS-SM 8 Port Packet Over SONET OC-3c/STM-1 100
8OC3X/POS-MM-MJ-B 8 port ISE OC3 105
16OC3/POS-SM 16 Port Packet Over SONET OC-3c/STM-1 100
16OC3X/POS-M-MJ-B 16 port ISE OC3 channelized DS3/E3 140
LC-1OC12/POS-SM 1 Port OC12/STM4 Packet Over SONET/SDH Line Card 80
EOS. 4 Port E.D. Packet Over SONET OC-12c/STM-4 100
4OC12/POS-IR-SC-B 4 Port Packet Over SONET OC-12c/STM-4 100
4OC12X/POS-M-SC-B 4 Port ISE Packet Over SONET OC-12c/STM-4 140
EOS. 1 Port E.D. Packet Over SONET OC-48c/STM-16 80
OC48E/POS-SR-SC-B 1 Port Packet Over SONET OC-48c/STM-16 78
OC48X/POS-LR-SC 1 Port ISE Packet Over SONET OC-48c/STM-16 140
OC192/POS-VSR 1 Port Packet Over SONET OC-192c/STM-64 174
LC-OC12-DS3 1 port SONET OC12 channelized to DS3 80
CHOC-12/STS3-IR-SC 1 port SONET OC12 channelized to STS3/STM-1 80
4CHOC12/DS3-IR-SC-B 4 port ISE OC12 channelized STS-3c/STM-1 or DS3/E3 140
CHOC48/DS3-IR-SC 1 port ISE OC48 channelized STS-12c/STM-4, STS-.. 140
6DS3-SMB-B 6 Port Packet over DS3 80
12DS3-SMB-B 12 Port Packet over DS3 80
4OC3/ATM-SM-SC 4 port ATM Over SONET OC-3c/STM-1 70
LC-1OC12/ATM-SM 1 port ATM Over SONET OC12c/STM-4c 62
4OC12/ATM-IR-SC 4 port ATM Over SONET OC12c/STM-4c 122
8FE-FX-SC-B 8 Port Fast Ethernet 77
GE-GBIC-SC-B 1 Port Gigabit Ethernet 65
3GE-GBIC-SC Cisco 12000 3 port Gigabit Ethernet 71
4GE-SFP-LC Cisco 12000 4 Port Gigabit Ethernet 106
OC12/SRP-IR-SC-B 1 Port SONET based SRP OC-12c/STM-4 80
OC48/SRP-LR-SC 1 Port SONET based SRP OC-48c/STM-16 100
12000-SIP-600 Cisco 12000 Series SPA Interface Processor-600 256
GSR04-FABRIC GSR 12404 Consolidated Fabric/Alarm Card 143
GSR6-CSC GSR 12406 Clock Scheduler Card 56
GSR6-SFC GSR 12406 Switch Fabric Card 45
GSR10-CSC GSR 12410 Clock Scheduler Card 19
GSR10-SFC GSR 12410 Switch Fabric Card 64
CSC-160,GSR12810 Clock Scheduler Card(10) OC-768 54
```

```
SFC-160,GSR12810 Switch Fabric Card(10) OC-768 107
GSR16/80-CSC Cisco 12016 80 Gbps GSR Clock Scheduler Card 43
GSR16/80-SFC Cisco 12016 80 Gbps GSR Switch Fabric Card 35
GSR16/320-CSC Cisco 12416 320 Gbps GSR Clock Scheduler Card 106
GSR16/320-SFC Cisco 12416 320 Gbps Switch Fabric Card 93
CSC-256,GSR12816 Clock Scheduler Card(16) OC-768 177
SFC-256,GSR12816 Switch Fabric Card(16) OC-768 151
GSR04-FABRIC Alarm Board(404) 208
GSR6-ALRM GSR 12406 Alarm Module 26
GSR10-ALRM GSR 12410 Alarm Module 33
GSR16-ALRM Cisco 12016 Alarm Module 35
GSR6-BLOWER GSR 12406 Blower Module 178
GSR16-BLOWER GSR 12016 Blower Module 178
Bus Board(16) 20
RP/0/0/CPU0:c12k#
```

If you plan to insert a new card, locate the entry for the card to be inserted and note the power it consumes. If this power is less than the figure given in Worst Case Redundant Power Available (the figure displayed in the **show environment power-supply table** command output), the card can be safely inserted. As long as the Worst Case Redundant Power Available is not zero, a PEM can be powered down for replacement without impact.

Note No alerts are issued if more cards are inserted than the PEMs can support. You are responsible for determining the power budget for the chassis before you change it. Exceeding the power budget can result in the PEM being overloaded and cards powering down due to insufficient available power.

Caveats

Caveats describe unexpected behavior in Cisco IOS XR software. A severity 1 caveat is the most serious; a severity 2 caveat is less serious. This section lists resolved, open, relevant caveats and the software module upgrade (SMU)s that resolves these caveats in Release 3.2.6.

Resolved Caveats

The following caveats from prior releases have been resolved in Cisco IOS XR Software Release 3.2.6.

- **CSCd68855**

  Brief Description: A loss of configuration can occur upon upgrade.

  Conditions: The configuration loss can occur because of a broken security banner that has been configured in alternate configuration mode.

  For example, if a customer has the following banner login config in the running-configuration:

```
banner login %
***** WARNING *****
This computer system is private and may be accessed only by authorized users. Data and
programs in this system are confidential and proprietary to the system owner and may
not be accessed, viewed, copied, reproduced, duplicated, modified, distributed, or
disclosed without authorization. Unauthorized users or users who exceed their
authorized level of access are subject to prosecution under state or federal law as
well as Company initiated proceedings
%
```

The preceding banner ends up as “banner login%” in the ASCII alternate-configuration. For example, you might see the following messages:

```
clock timezone MET 1
clock summer-time MET recurring last sunday march 02:00 last sunday october 03:00
banner motd %
telnet ipv4 server max-servers 10
```

Workaround: Remove any banner commands, such as “banner login” or “banner motd,” before performing an upgrade. After the upgrade has finished, reapply your banner configuration lines.

- **CSCuk60349**

  Brief Description: The maximum transfer unit (MTU) on a bundled Packet-Over-SONET (POS) interface is removed when an RP fails over.

  Conditions: If no intf-owner MTU configuration verification is made on the standby RP, the default action is to reject the configuration. The result is that the MTU configuration is subsequently missing after an RP failover.

  Workaround: None

- **CSCsd47241**

  Brief Description: OC192 RX PKT LED is not blinking on Port 0 and Port 2 while packets arrive.

  Conditions: Problem occurs on a 4-port OC-192c/STM-64c POS/DPT PLIM that is running Release 3.2.2 or a later release. (Release 3.2.1 does not have this problem.)

  Workaround: None

- **CSCsd63325**

  Brief Description: The discovery process is not spawned on standby board (RP, DRP).

  Symptom: The discovery process, which collects DRAM errors, peripheral component interconnect (PCI) bus errors, and so on, must run on the standby card (RP, DRP). Today, the system error on the standby card is reported when the board is becoming active. This causes the system to fail. Two applicable DRAM bits apply to this failure: error correcting codes (ECC) and PCI.

  Conditions: This causes a problem only when the standby RP is affected by a hardware failure.

  Cisco IOS XRWorkaround: None

- **CSCse79437**

  Brief Description: Message appears: “SECURITY-LOCALD-4-ACCT_FAILURE after IOS XR upgrade with no TACACS server.”

  Symptom: The following log message can be seen in a Cisco CRS-1 router after an upgrade of Cisco IOS XR software:

  locald[241]: %SECURITY-LOCALD-4-ACCT_FAILURE: Failed to send the accounting record - retry limit exceeded and the request will be dropped.

  Conditions: This error occurs when a customer is using a TACACS+ server for authentication on the Cisco CRS-1 router.

  Workaround: The workaround is to restart the local process on the router.

- **CSCsd79544**

  Brief Description: Software fails to send an SNMP trap for the CISCO-SENSOR-MIB.

Conditions: Software fails to send an SNMP trap for the CISCO-SENSOR-MIB when any thresholds are reached for the environmental process in Release 3.2.3. The Cisco CRS-1 router (and likely the Cisco XR 12000 Series Router) fails to send an SNMP trap when any thresholds are reached for the envmon process under Release 3.2.3 and also the latest Release 3.3.x builds. The device does generate alarms through syslog, however.

Workaround: A workaround is to use syslog messages for alarming environment issues.

- **CSCei77075**

  Brief Description: The following message might appear:

  "Failed to wrlock CM conn rwlock."

  Symptom: SYSDB-SYSDB-3-LOCKING log messages might appear on a Cisco CRS-1 router.

  Conditions: This error occurs on a Cisco CRS-1 router that is running Cisco IOS XR software.

  Workaround: Restart the sysdb_mc process on the node that is putting out this error.

- **CSCsd02952**

  Symptom: TE tunnel label goes unlabeled after RP switchover if graceful restart has been enabled.

  Brief Description: When RP switchover is performed on the Cisco CRS-1 router with both non-stop forwarding (NSF) and Resource Reservation Protocol (RSVP) graceful restart enabled, MPLS TE tunnel on the remote router (NSF aware) that uses RP failover router as the tunnel tail flaps. It causes traffic loss up to 30 seconds.

  Conditions: All of the following conditions are present:

  – NSF and RSVP graceful restart are enabled.

  – TE tunnel is established on a broadcast medium such as GE.

  – RP failover is performed on tunnel tail.

  Workaround: Change the IGP network interface type to Point-To-Point.

- **CSCsd10378**

  Brief Description: IS-IS cannot create bidirectional forwarding detection (BFD) session after RP fail over and LC OIR because protocols that use BFD fail to create their BFD sessions.

  Conditions: This problem might happen after an RP failover or an LC reload.

  Workaround: Restart the BFD process on an RP: "process restart bfd."

- **CSCsd85267**

  Brief Description: Traffic is lost after RP failover.

  Symptom: After failover with nongraceful restart configured for label distribution protocol (LDP) and no graceful restart for a TE is configured.

  Conditions: MPLS forwarding entries are not correct on a LC. Some of the label entries have some invalid outgoing paths or nexthops in their load balance o/p data structure, so they do not match MPLS forwarding entries on the RP in the control plane LDP or Label Switching Database (LSD).

  Potential fix of the issue:

  LSD does not allow clients like LDP to connect and send requests to LSD if the transport to the Label Forwarding Database (LFD) is not yet available.

  Workaround: None

- **CSCse00294**

  Brief Description: Tag 2 IP paths lose traffic after a no shut of an interface with Release 3.2.x.

Conditions: After an interface shutdown, the address resolution protocol (ARP) entries on that interface are removed, and then IPv4 and MPLS adjacency entries are removed. If the interface is no shut and if MPLS traffic is flowing, no ARP request is generated and traffic is dropped. An ARP request is sent only when an attempt is made to forward IPv4 traffic out from the interface.

Workaround: Use static ARP entries. In addition, this fix ensures that an MPLS packet is pushed to Netio and an IPv4 ARP request is generated.

- **CSCse23802**

  Brief Description: The RSVP process fails upon an **show rsvp session detail** execution if either the Path or RESV message has more than 20 Record Route Option (RRO) subobjects.

  The log shows MALLOC_ERROR as the RSVP process fails.

  Conditions: (Observed with Release 3.2.3.)

  The failure is specific to the **show rsvp session detail** command and happens if either the Path or Resv message contains more than 20 RRO subobjects.

  For Path messages, the number of nodes in the topology refers to nodes that are upstream from a Cisco CRS-1 router.

  Workaround: Do not use the s**how rsvp session detail** command.

- **CSCek42760**

  Brief Description: The system fails to the boot minimum boot image (MBI) after system is powered off and on.

  Symptom: The system does not boot after power is turned off and on. RP constantly reboots.

  Workaround: Boot with one RP installed.

- **CSCse12144**

  Brief Description: System cannot boot after power is turned off and on.

  Symptom: System cannot boot after power is turned off and on. RP appears to constantly reboot.

  Conditions: This problem has been observed with Release 3.2.3 or Release 3.2.4.

  Workaround: Connect console connection to AUX port. After the RP resets, wait until prompted for username and password. Log in with a locally authenticated username. At the command prompt, enter the **reboot** command. The system reloads and, in most instances, boots correctly. If the system does not reboot correctly, repeat the procedure.

- **CSCse40388**

  Brief Description: Null TLU2 entry when an IGP Equal Cost Multipath Protocol （ECMP) to BGP next-hop address exists.

  Symptom: On a Cisco CRS-1 router or MC, a packet destined to a specific address is dropped due to Null TLU2 entry in LC hardware egress CEF table.

  Conditions: The problem occurs when both the following conditions are true:

  A packet follows the BGP path

  That packet encounters an IGP Equal Cost Multipath Protocol (ECMP) to BGP next-hop address.

  Workaround: Take the following steps:

  1. Add a static route for the destination address.
  2. Clear the route entry.
  3. Eliminate IGP ECMP by adjusting the IGP cost.

Note The problem reoccurs if the route entry is simply cleared.

- **CSCek25587**

  Brief Description: The bound addresses for a remote peer went missing when the peer's router-ID changed.

  Symptom: Unit under test (UUT) is the router running Cisco IOS XR software. After the router ID of a neighbor changes, the address binding error messages appear on UUT. UUT has no addresses for the neighbor, so any traffic directed to the neighbor goes only to the IP (unlabeled).

  Conditions: LDP does not handle address binding advertisement correctly when a change to the neighbor router ID causes a peer session to flap, causing a new peer session to come up (and advertise address bindings), while the previous peer session (with the old router ID) is in the process of being cleaned up.

  Workaround: Restart the LDP process or clear the affected given LDP session by using the **mpls ldp restart session** command**.**

- **CSCsd18900**

  Brief Description: Process statsd_server is blocked by Group Services Protocol (GSP).

  Symptom: Various processes become blocked by GSP, causing service loss over the affected node.

  Conditions: This problems follows an RP failover.

  Workaround: Restart the GSP process on the affected node by using the **process restart gsp locatio**n *location of the node* command.

- **CSCei57651**

  Brief Description: IP connectivity problem occurs after reload.

  Symptom: Ping fails after reload, seen intermittently.

  Conditions: Problem intermittently occurs after a reload.

  Workaround: Restart the adjacency information base (AIB) to restore connectivity.

- **CSCek43161**

  Brief Description: Umbrella DDTS for CSCsd53847 and CSCsd89508.

  This DDTS addresses two issues:

  1. The ifPhysAddr object identifier registry (OID) within the IF-MIB is not populated and returns a null value.
  2. SNMP GET BULK operations may fail when the response protocol data unit (PDU) is greater than the default size.

  Conditions: Condition No. 1 is seen in regular operation. Condition No. 2 is seen if a nondefault value is set through the **snmp-server packetsize** command.

  Workaround: Workaround for condition No. 2 is to remove the **snmp-server packetsize** configuration and return it to the default.

- **CSCsd34953**

  Brief Description: A message of noSuchName on OID is returned upon a query MIBCiscoPingTable 1.3.6.1.4.1.9.9.16.1.1.1.14.

  Symptom: A first get request answer returns a "no such name" message, but the second get request returns the answer.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SNMPv2c::getrequest("aaa.bbb.ccc.ddd", "xxxxRO",
"1.3.6.1.4.1.9.9.16.1.1.1.14.1279769442")
= (129, 0, 1.3.6.1.4.1.9.9.16.1.1.1.14.1279769442);
Error 2: No Such Name
sleep(1)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

A second getrequest provides the result.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SNMPv2c::getrequest("aaa.bbb.ccc.ddd", "xxxxRO",
"1.3.6.1.4.1.9.9.16.1.1.1.14.1279769442")
= (2, 1, 1.3.6.1.4.1.9.9.16.1.1.1.14.1279769442);
```

Workaround: None.

- **CSCek42149**

  Brief Description: If the second link in ECMP load balancing receives a **no shutdown** command, traffic is diverted to this link and dropped for a second, until ARP is resolved.

  Conditions:

  Traffic to the destination address that is made available by issuing a **no shutdown** command to the link is already flowing over a different link. Bringing up the new link causes routing protocols to divert some traffic over the link. No ARP entry exists for the next-hop address over the new link, so a delay occurs in resolving the address, which results in packet loss.

  Workaround: Configure a static ARP entry for the adjacency on the interface that provides a second ECMP path and is expected to flap.

In addition to the DDTS items just described, Table 7 contains DDTSs (which are released as SMUs in previous maintenance releases) that are also resolved in Release 3.2.6.

Table 7 SMUs That Are Resolved and Included in Release 3.2.6

SMU ID	SMU/Image Name	DDTS	Symptom
AA01433	hfr-base-3.2.3.CSCei57651	CSCei57651	IP connectivity problem after reload.
AA01376	hfr-mpls-3.2.2.CSCek25587	CSCek25587	Bound addresses are missing for remote peer when peer changed router-ID.
AA01520	hfr-base-3.2.3.CSCek42149	CSCek42149	A **no shutdown** command on 10GE in load balancing causes traffic loss.
AA01487	hfr-base-3.2.3.CSCek42760	CSCek42760	System failed to boot MBI after system is powered off and on.
AA01488	hfr-base-3.2.4.CSCek42760	CSCek42760	System failed to boot MBI after system is powered off and on.
AA01493	hfr-base-3.2.2.CSCek43161	CSCek43161	Umbrella DDTS for CSCsd53847 and CSCsd89508.
AA01375	hfr-mpls-3.2.2.CSCsd02952	CSCsd02952	TE tunnel label goes unlabelled after RP switchover with GR setting.
AA01404	hfr-base-3.2.3.CSCsd10378	CSCsd10378	IS-IS cannot create BFD session after RP failover and LC OIR.
AA01465	hfr-base-3.2.3.CSCsd18900	CSCsd18900	statsd_server is blocked by GSP.

Table 7 SMUs That Are Resolved and Included in Release 3.2.6 (continued)

AA01412	hfr-mgbl-3.2.2.CSCsd34953	CSCsd34953	noSuchName on OID query MIBCiscoPingTable 1.3.6.1.4.1.9.9.16.1.1.1.14.
AA01437	hfr-os-mbi-3.2.2.CSCsd63325	CSCsd63325	Discovery process not spawned on standby board (RP, DRP).
AA01436	hfr-os-mbi-3.2.3.CSCsd63325	CSCsd63325	Discovery process not spawned on standby board (RP, DRP).
AA01435	hfr-os-mbi-3.2.4.CSCsd63325	CSCsd63325	Discovery process not spawned on standby board (RP, DRP).
AA01427	hfr-base-3.2.2.CSCsd68855	CSCsd68855	Configuration lost due to a broken security banner that was configured in alternate configuration mode.
AA01428	hfr-base-3.2.3.CSCsd68855	CSCsd68855	Configuration lost due to a broken security banner that was configured in alternate configuration mode.
AA01429	hfr-base-3.2.4.CSCsd68855	CSCsd68855	Configuration lost due to a broken security banner that was configured in alternate configuration mode.
AA01443	hfr-admin-3.2.3.CSCsd79544	CSCsd79544	CISCO-SENSOR-MIB traps not functional.
AA01462	hfr-base-3.2.2.CSCsd80950	CSCsd80950	Umbrella DDTS for CSCsd46034, CSCsd53847, CSCek29773.
AA01448	hfr-mpls-3.2.2.CSCsd83826	CSCsd83826	Umbrella DDTS for invalid packet handling.
AA01444	hfr-mpls-3.2.3.CSCsd83826	CSCsd83826	Umbrella DDTS for invalid packet handling.
AA01449	hfr-mpls-3.2.4.CSCsd83826	CSCsd83826	Umbrella DDTS for invalid packet handling.
AA01464	hfr-mpls-3.2.3.CSCsd85267	CSCsd85267	Traffic loss after RP failover.
AA01475	hfr-mpls-3.2.3.CSCse00294	CSCse00294	tag2ip paths have traffic loss after a **no shutdown** command is issued to an interface with Release 3.2.3.
AA01479	hfr-base-3.2.3.CSCse12144	CSCse12144	System failed to boot MBI after system is powered off and on.
AA01486	hfr-base-3.2.4.CSCse12144	CSCse12144	System failed to boot MBI after system is powered off and on.
AA01503	hfr-mpls-3.2.3.CSCse23802	CSCse23802	RSVP fails upon a **show rsvp session detail** command if Path or RESV message has more than 20 RRO subobjects.

Table 7 SMUs That Are Resolved and Included in Release 3.2.6 (continued)

AA01524	hfr-mpls-3.2.3.CSCse76535	CSCse76535	RSVP: process restarts while processing policy.
AA01409	hfr-base-3.2.3.CSCuk60349	CSCuk60349	If no intf-owner MTU configuration verification is made on the standby RP, the default action is to reject the configuration. The result is that the MTU configuration is subsequently missing after an RP failover.

Open Caveats—Release 3.2.6

None.

Upgrade Instructions for Release 3.2.6

This section describes an upgrade on a Cisco CRS-1 router and Cisco XR 12000 Series Router. (Note that a Cisco XR 12000 Series Router does not run Release 3.2.6.) The information lists show required and optional software packages and, for the Cisco CRS-1 router, instructions for activating a SMU.

Commands and Tasks for Upgrading Software

This section has URLs for information you need to upgrade or downgrade the software. The topics are:

- Obtaining required PIE files
- Checking for mandatory SMUs
- Checking the system stability
- Performing pre-upgrade tasks
- Upgrading the software
- Downgrading the software
- Post-upgrade and post-downgrade procedures

For a Cisco CRS-1 router, go to:

http://www.cisco.com/cgi-bin/tablebuild.pl/crs1upgrade

For a Cisco XR 12000 Series Router, go to:

http://www.cisco.com/cgi-bin/tablebuild.pl/c12000upgrade

Upgrade Instructions for the Cisco CRS-1 Router

This section lists the required and optional files for a Cisco CRS-1 Release 3.2.6 upgrade. A name might differ from an actual filename because names can change. The filenames you use do not affect operation.

Table 8 Required and Optional Packages for Upgrading from Release 3.2.x to Release 3.2.6 on Cisco CRS-1 Routers

PIE File Description	Sample PIE Filename	Sample Package Name
Required Package		
Composite mini-package (OS-MBI, base, administration, forwarding, LC route)	comp-hfr-mini.pie-3.2.6	disk0:comp-hfr-mini-3.2.6
Optional Individual Packages[1]		
Multicast Package	hfr-mcast.pie-3.2.6	disk0:hfr-mcast-3.2.6
Manageability Package	hfr-mgbl.pie-3.2.6	disk0:hfr-mgbl-3.2.6
MPLS Package	hfr-mpls.pie-3.2.6	disk0:hfr-mpls-3.2.6
Security Package	hfr-k9sec.pie-3.2.6	disk0:hfr-k9sec-3.2.6

1. Packages are installed individually.

Steps for the Required SMUs for Upgrading a Cisco CRS-1 Router

The steps for adding and activating the required SMU for upgrading from Cisco IOS XR Software Release 3.2.0 to Release 3.2.x in the Cisco CRS-1 router appear in Table 9.

The steps for adding and activating the required SMU for upgrading from Cisco IOS XR Software Release 3.2.x to Release 3.2.6 in the Cisco CRS-1 router appear in Table 10.

Table 9 Required SMU for Upgrading From 3.2.0 to 3.2.x on Cisco CRS-1 Routers

SMU filename	hfr-base-3.2.0.CSCei45039.pie
DDTS	CSCei45039
Problem summary	Configuration loss during upgrade from release 3.2.0 to 3.2.x
SMU installation impact	Low—no impact to running system.
SMU install procedure	1. Add SMU: (admin)# **install add <hfr-base-3.2.0.CSCei45039.pie> to disk0:** 2. Activate SMU: (admin)# **install activate disk0:hfr-base-3.2.0.CSCei45039-1.0.0** 3. Trigger the SMU by committing the configuration: # **config** (config)# **hostname** *same-hostname* (config)# **commit** (config)# **exit** 4. Commit the SMU: (admin)# **install commit**

Table 10 Required SMU for Upgrading From Release 3.2.x to Release 3.2.6 on Cisco CRS-1 Routers

SMU filename	hfr-base-3.2.x.CSCsd68855.pie (The x can be 0, 1, 2, 3, or 4.)
DDTS	CSCsd68855
Problem summary	Configuration loss on upgrade caused by broken banner configuration in alternate configuration.
SMU installation impact	Low—no impact should occur to a running system.
SMU Package Name	<boot device>hfr-base-3.2.x. CSCsd68855-1.0.0 (The x can be 0, 1, 2, 3, or 4.)
SMU install procedure	1. Add the SMU: router(admin)# **install add <hfr-base-3.2.x.CSCsd68855.pie> to disk0:** 2. Activate the SMU: router(admin)# **install activate disk0:hfr-base-3.2.x.CSCsd68855-1.0.0** (The x can be 0, 1, 2, 3, or 4.) 3. Trigger the SMU by committing the configuration: # **config** (config)# **hostname** *same-hostname* (config)# **commit** (config)# **exit** 4. Commit the SMU: (admin)# **install commit**

Special Upgrade Instructions

This section contains any applicable special instructions for upgrading from Cisco IOS XR Software Release 3.2.x to Release 3.2.6.

None

Special Downgrade Instructions

This section contains any applicable special instructions for downgrading from Cisco IOS XR Software Release 3.2.6 to Release 3.2.x.

None

Caveats

This section contains any caveats for an upgrade from Cisco IOS XR Software Release 3.2.x to Release 3.2.6.

None

Upgrade Instructions for Cisco XR 12000 Series Routers

This section contains one table, Table 11. It lists the required and optional packages.

Table 11 Required and Optional Packages for Upgrading From 3.2.x to 3.2.3 on Cisco XR 12000 Series Routers

PIE File Description	Sample PIE Filename	Sample Package Name
Required Package		
Composite mini package (OS-MBI, base, administration, forwarding, LC route)	comp-c12k-mini.pie-3.2.3	disk0:comp-c12k-mini-3.2.3
Optional Individual Packages[1]		
Multicast Package	c12k-mcast.pie-3.2.3	disk0:c12k-mcast-3.2.3
Manageability Package	c12k-mgbl.pie-3.2.3	disk0:c12k-mgbl-3.2.3
MPLS Package	c12k-mpls.pie-3.2.3	disk0:c12k-mpls-3.2.3
Security Package	c12k-k9sec.pie-3.2.3	disk0:c12k-k9sec-3.2.3

1. Packages are installed individually.

Mandatory SMUs

This section contains possible information for mandatory SMUs for the Cisco XR 12000 Series Router. The following SMUs are required prior to upgrade (for upgrading from Cisco IOS XR Software Release 3.2.0, Release 3.2.1, or Release 3.2.2 to Release 3.2.3).

None

Special Upgrade Instructions

This section contains special instructions for mandatory SMUs for the Cisco XR 12000 Series Router:

Please follow these special instructions during upgrade (for upgrading from Cisco IOS XR Software Release 3.2.0, Release 3.2.1, Release or 3.2.2):

None

Special Downgrade Instructions

This section contains possible special instructions for downgrading software (to Cisco IOS XR Software Release 3.2.0, Release 3.2.1, or Release 3.2.2) on a Cisco XR 12000 Series Router.

None

Caveats

This section contains possible caveats for upgrading software on a Cisco XR 12000 Series Router (from Cisco IOS XR Software Release 3.2.0, Release 3.2.1, or Release 3.2.2).

None

Troubleshooting

See *Cisco IOS XR Getting Started Guide* for information on troubleshooting the Cisco IOS XR software.

Related Documentation

The following sections describe the documentation available for the Cisco CRS-1 and Cisco XR 12000 Series Router. These documents consist of hardware and software installation guides, Cisco IOS XR software configuration and command references, feature modules, and other documents.

Documentation is available as electronic documents, which are available online on Cisco.com.

Use these release notes with these documents:

- Hardware Documents, page 25
- Software Documents, page 25

Hardware Documents

You can find the most current hardware documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/crs/index.htm

Software Documents

The Cisco IOS XR software documentation set consists of the Cisco IOS XR software configuration guides and command references, a getting started guide, and other supporting documents. Refer to the *About Cisco IOS XR Software Documentation for Release 3.2* for a list of Cisco IOS XR software documentation for Release 3.2.6.

You can find the most current software documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/crs/index.htm

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

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

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has defined these severities:

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

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