



# Release Notes for Cisco 7000 Family for Cisco IOS Release 11.1 CA

---

**February 24, 2002**

Cisco IOS Release 11.1(36)CA3

78-3799-24 C0

These release notes for the Cisco 7000 family of routers support Cisco IOS Release 11.1(36)CA3. These release notes are updated to describe new memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 11.1 CA, see the [“Caveats” section on page 24](#) and the *Release Notes for Cisco IOS Release 11.1*. The document *Release Notes for Cisco IOS Release 11.1* is updated for every maintenance release and is located on Cisco Connection Online (CCO) and on the Documentation CD-ROM.

Cisco IOS Software Release 11.1CA has achieved general deployment (GD) on Cisco 7200, 7500, and RSP7000-based 7000 platforms, beginning with Cisco IOS maintenance Release 11.1(22)CA. For more information, see the *General Deployment (GD) Announcement for Cisco IOS Software Release 11.1CA on Cisco 7200 and 7500 Platforms*.

## Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [MIBs, page 18](#)
- [Important Notes, page 19](#)
- [Caveats, page 24](#)
- [Related Documentation, page 53](#)
- [Obtaining Documentation, page 57](#)
- [Obtaining Technical Assistance, page 58](#)



- [Open Source License Acknowledgements, page 60](#)

## System Requirements

This section describes the system requirements for Release 11.1(36)CA3 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 3](#)
- [Microcode, page 3](#)
- [Feature Sets, page 4](#)

## Memory Requirements

[Table 1](#) describes the memory requirements for the feature sets for the Cisco 7000 family of routers supported by Cisco IOS Release 11.1 CA.

- For port adapter hardware and memory configuration guidelines for the Cisco 7200 series routers, refer to the document *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines*.
- Cisco 7500 series routers require a 16- or 20-MB Flash memory card to support the Enterprise/APPN/VIP feature set and the Channel Interface Processor (CIP) microcode.

**Table 1** Memory Recommendations for Cisco 7000 Family Routers

Platforms	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
<b>Cisco 7200 series routers</b>	Enterprise	c7200-j-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise/APPN	c7200-aj-mz	8 MB Flash	32 MB DRAM	RAM
	Desktop/IBM	c7200-dr-mz	8 MB Flash	32 MB DRAM	RAM
	Network Layer 3 Switching	c7200-inu-mz	8 MB Flash	16 MB DRAM	RAM
<b>Cisco 7500 series and Cisco 7000 series routers with RSP7000 and RSP7000CI</b>	Enterprise	rsp-j-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise/APPN	rsp-aj-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise/APPN/VIP	rsp-ajv-mz	16 MB Flash	32 MB DRAM	RAM
	Enterprise/VIP	rsp-jv-mz	16 MB Flash	32 MB DRAM	RAM

## Supported Hardware

Cisco IOS Release 11.1 CA supports the following platforms:

- Cisco 7500 series routers
- Cisco 7200 series routers
- Cisco 7000 series routers with the RSP7000 and RSP7000CI

Refer to the *Release Notes for Cisco IOS Release 11.1* publication for a summary of the LAN interfaces supported on each platform and the WAN data rates and interfaces supported on each platform.

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software c7200-dr-mz, Version 11.1(36)CA3, RELEASE SOFTWARE
```

## Microcode

Microcode software images are bundled with the system software image—with the exception of the Channel Interface Processor (CIP) microcode (all system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. [Table 2](#) lists the current microcode versions for Cisco 7000 family routers.

**Table 2** Current Microcode Versions for Cisco 7000 Family Routers

Processor or Module	Current Bundled Route Switch Processor Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	20.5
EIP (Ethernet Interface Processor)	20.6	20.1
FEIP (Fast Ethernet Interface Processor)	20.8	20.1
FIP (FDDI Interface Processor)	20.4	20.1
FSIP (Fast Serial Interface Processor)	20.9	20.1
HIP (HSSI Interface Processor)	20.2	20.0
MIP (MultiChannel Interface Processor)	22.3	20.3
POSIP (Packet over SONET OC-3 Interface Processor)	20.1	20.0
TRIP (Token Ring Interface Processor)	20.2	20.0
VIP (Versatile Interface Processor)	21.40	21.9
VIP2 (second-generation Versatile Interface Processor)	21.40	21.40

## Feature Sets

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.



### Caution

Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

The following feature sets are supported by Cisco IOS Release 11.1(36)CA3 for Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers. Refer to the *Release Notes for Cisco IOS Release 11.1* publication for a complete list of the features provided in these sets.

Feature sets for Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI are:

- Enterprise (rsp-j-mz image)
- Enterprise/APPN (rsp-aj-mz image)
- Enterprise/VIP (rsp-jv-mz image)
- Enterprise/APPN/VIP (rsp-ajv-mz image)

Feature sets for Cisco 7200 series routers are:

- Enterprise (c7200-j-mz image)
- Enterprise/APPN (c7200-aj-mz image)
- Desktop/IBM (c7200-dr-mz image)
- Network Layer 3 Switching (c7200-inu-mz image)

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Release 11.1 CA.

### New Features in Release 11.1(36)CA3

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(36)CA3.

### New Features in Release 11.1(36)CA2

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(36)CA2.

## **New Features in Release 11.1(36)CA1**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(36)CA1.

## **New Features in Release 11.1(36)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(36)CA.

## **New Features in Release 11.1(34)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(34)CA.

## **New Features in Release 11.1(32)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(32)CA.

## **New Features in Release 11.1(30)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(30)CA.

## **New Features in Release 11.1(28)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(28)CA.

## **New Features in Release 11.1(26)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(26)CA.

## **New Features in Release 11.1(24)CA**

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(24)CA.

## New Features in Release 11.1(22)CA

There are no new features for Cisco 7000 series routers, Cisco 7200 series routers, and Cisco 7500 series routers in Cisco IOS Release 11.1(22)CA.

## New Hardware Features in Release 11.1(20)CA1

The following new hardware feature has been added to Release 11.1(20)CA1:

### PA-4R-DTR Dedicated Token Ring Port Adapter

The Dedicated Token Ring port adapter (PA-4R-DTR) is available on Cisco 7500 series routers, Cisco 7200 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-4R-DTR provides up to four IBM Token Ring or IEEE 802.5 Token Ring interfaces. Each Token Ring interface can be set for 4-Mbps or 16-Mbps half-duplex or full-duplex operation and can operate as a standard Token Ring station or as a concentrator port. The default for all interfaces is Token Ring station mode with half-duplex, 16-Mbps operation. The PA-4R-DTR connects over Type 1 or Type 3 lobe cables, with each interface providing an RJ-45 receptacle.

## New Hardware Features in Release 11.1(20)CA

The following new hardware feature has been added to Release 11.1(20)CA:

### Second-Generation Fast Ethernet Interface Processors

The FEIP2-DSW second-generation Fast Ethernet Interface Processor is a replacement for the FEIP2-2TX and FEIP2-2FX, available on Cisco 7500 series routers and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Software Features in Release 11.1(20)CA

The following new software feature has been added to Release 11.1(20)CA:

### Web Cache Control Protocol Command Enhancements

The following changes were made to Web Cache Control Protocol (WCCP) commands:

- The **ip wccp** command is now the **ip wccp enable** command.
- The **ip wccp redirect-list** command was added.
- The output of the **show ip wccp** command was modified to include access list information.

## New Hardware Features in Release 11.1(18)CA

The following new hardware feature has been added to Release 11.1(18)CA:

### CSA Support over HSSI

SA-Comp/1 and SA-Comp/4 data Compression Service Adapters (CSAs) now operate over High-Speed Serial Interface (HSSI) links available through the PA-2H and PA-H Revision B port adapters. When using compression, limit HSSI speeds to 16 Mbps to ensure no packet loss.

## New Hardware Features in Release 11.1(17)CA

The following new hardware feature has been added to Release 11.1(17)CA:

### RJ-45 Interface Support

Cisco 7200 series routers support a new I/O controller with an RJ-45 interface. The optional Fast Ethernet port is configurable for use at 100 Mbps full-duplex or half-duplex (half duplex is the default). The Fast Ethernet port is equipped with either a single MII receptacle or an MII receptacle and an RJ-45 receptacle.

To support this new feature, the **media-type** interface command has been modified. The **media-type** interface command now supports two options:

- **100basex**—Specifies an RJ-45 100BaseX physical connection
- **mii**—Specifies a media-independent interface

**Note**

---

When you use the I/O controller that is equipped with an MII receptacle and an RJ-45 receptacle, only one receptacle can be configured for use at a time.

---

## New Software Features in Release 11.1(17)CA

The following new software feature has been added to Release 11.1(17)CA:

### NetFlow Switching Enhancements

The new **ip flow-cache active-timeout** configuration command lets you specify the timeout period for the NetFlow cache.

## New Hardware Features in Release 11.1(16)CA

The following new hardware feature has been added to Release 11.1(16)CA:

### Channelized T3 Dual-Wide Port Adapter

The channelized T3 dual-wide port adapter (PA-CT3/4T1) is available on Cisco 7200 series routers.

## New Software Features in Release 11.1(16)CA

The following new software features have been added to Release 11.1(16)CA:

### VIP Enhancements

New privileged EXEC commands provide more information about the Versatile Interface Processor (VIP). The **show controllers logging** command displays logging information about a VIP. The **show controllers tech-support** command displays general information about a VIP while reporting a problem. The **show controllers align** command shows NULL pointer dereferences and misaligned accesses for a VIP.

### POS Command Enhancement

The new **pos scramble-atm** interface command enables SONET payload scrambling on a Packet-over-SONET (POS) interface. SONET payload scrambling applies a self-synchronous scrambler ( $x^{43}+1$ ) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density.

### Distributed Switching for LANE

In LAN Emulation (LANE) networks, distributed switching for LANE is a new Cisco 7500 series feature that allows a LAN Emulation Client (LEC) to be distributed from the RSP to one or more VIP2 interfaces. In doing so, the VIP2 distributed switching capability can now provide switching between each emulated LAN connected to each VIP2 independently. This ability provides increased aggregate IP switching performance across the Cisco 7500 architecture for LANE networks versus centralized Route Switch Processor (RSP) switching. The inter-ELAN switching performance provided by the VIP2 modules is additive across the Cisco 7500 series routers and increases with each new VIP2/ATM port adapter. This ability also minimizes the utilization of the RSP—freeing the RSP for other functions, including low-level routing and routing updates.

The other components of LANE, such as LAN Emulation Server (LES), broadcast and unknown server (BUS), and LAN Emulation Configuration Server (LECS), are functions used primarily during network initialization for address lookups. These functions are not in the data flow, and distributing these functions does not provide any performance gain. Therefore, the LES, BUS, and LECS functions continue to reside on the RSP with this feature.

Distributed switching for LANE for Cisco 7500 series routers complies completely with ATM Forum standards. It is intended for any enterprise or ISP ATM applications in which multiple VIP2/ATM port adapter combinations are installed in the same Cisco 7500 series router, or for any ATM applications where the performance can be optimized by dedicating the RSP to other routing functions.

This capability only supports IP for Ethernet LANE in a distributed manner. Token Ring LANE is not supported through distributed switching; however, it is supported within the RSP.

## LANE Optimum Switching Enhancement

Optimum switching is now supported for LANE traffic on the RSP.

## New Hardware Features in Release 11.1(15)CA

The following new hardware features have been added to Release 11.1(15)CA:

### PA-T3 and PA-2T3 Serial Port Adapter

The PA-T3 and PA-2T3 serial port adapters are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). For information on interoperability guidelines for T3 serial port adapter data service units (DSUs), refer to the *T3 Serial Port Adapter Installation and Configuration* publication that ships with the product.

### VIP2-50

The VIP2-50 is available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). Although the VIP2-50 is being announced with Release 11.1(15)CA, it is also supported in Release 11.1(14)CA1.

### High-Speed Serial Interface Port Adapters

The PA-2H Revision B port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). This port adapter was revised to improve performance.

### Channelized T3 Interface Processor Feature Enhancements

The Channelized T3 Interface Processor (CT3IP) available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) now supports the following types of remote line Facility Data Link (FDL) loopback:

- FDL ANSI loopback per ANSI T1.403
- FDL Bellcore loopback per TR-TSY-000312

## New Software Features in Release 11.1(15)CA

The following new software feature has been added to Release 11.1(15)CA:

### NetFlow Switching Enhancements

The NetFlow switching commands have been modified to provide added functionality. The **ip flow-export destination**, **ip flow-export source**, and **ip flow-export version** commands replace the **ip flow-export** command.

## New Hardware Features in Release 11.1(14)CA

The following new hardware feature has been added to Release 11.1(14)CA:

### PA-A2 ATM-CES Port Adapter Enhancements

The PA-A2 ATM-CES port adapters (PA-A2-4T1C-OC3SM, PA-A2-4T1C-T3ATM, PA-A2-4E1XC-OC3SM, PA-A2-4E1XC-E3ATM, PA-A2-4E1YC-OC3SM, and PA-A2-4E1YC-E3ATM) available on Cisco 7200 series routers now support the following new features:

- Available bit rate (ABR)—The ABR service category is specified in the ATM Forum Traffic Management Specification Version 4.0.
- Virtual path shaping—A virtual path (VP) is a logical association or bundle of virtual circuits (VCs).

In addition, all traffic shaping features available with the **atm pvc** interface command (*peak average burst*) are supported, and you can now configure the number of transmit channels for the interface with the **atm tx-channels** interface configuration command.

## New Software Features in Release 11.1(14)CA

The following new software features have been added to Release 11.1(14)CA:

### Fast EtherChannel

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel can be configured between Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP700CI and a Catalyst 5000 switch.

### Web Cache Control Protocol

The Web Cache Control Protocol feature transparently redirects HTTP requests from the intended server to a Cisco Cache Engine. When the Cisco Cache Engine receives the request, it attempts to service the request from its own cache. If the requested information is not present, the Cisco Cache Engine then makes a request to the Web server to get the required information. After receiving the required information from the Web server, the Cisco Cache Engine passes the information back to the client and possibly caches it to fill future requests.

## New Hardware Features in Release 11.1(13)CA1

The following new hardware features have been added to Release 11.1(13)CA1:

### PA-E3 and PA-2E3 Serial Port Adapters

The PA-E3 and PA-2E3 serial port adapters are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). For information on interoperability guidelines for E3 serial port adapter data service units (DSUs), refer to the *E3 Serial Port Adapter Installation and Configuration* publication that ships with the product.

### NPE-200 Network Processing Engine for Cisco 7200 Series Routers

The NPE-200 for Cisco 7200 series routers is now available. The network processing engine maintains and executes the system management functions for Cisco 7200 series routers. The network processing engine also shares the system memory and environmental monitoring function with the I/O controller. The NPE-200 has an R5000 microprocessor that operates at an internal clock speed of 200 MHz, 4 MB of SRAM, and erasable programmable read-only memory (EPROM) for storing sufficient code for booting the Cisco IOS software.

## New Software Features in Release 11.1(13)CA1

The following new software feature has been added to Release 11.1(13)CA1:

### NetFlow Switching Enhancements

The NetFlow switching commands have been modified to provide added functionality and improved performance under heavy traffic conditions. Netflow switching is a high-performance, network-layer switching path that captures as part of its switching function a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service information that can be used for a wide variety of purposes such as network analysis and planning, accounting, and billing.

NetFlow switching is supported on IP and IP encapsulated traffic over all interface types and encapsulations except for ISL/VLAN, ATM and Frame Relay interfaces when more than one input access control list is used on the interface, and ATM LANE.

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow switching, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a “connection-oriented” basis as part of the flow, where access list checks are bypassed and packet switching and statistics capture are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a give source and destination--both defined by a network-layer IP address and transport-layer port number. Specifically, a flow is identified as the combination of the following fields:

- source IP address
- destination IP address
- source port number

- destination port number
- protocol type
- type of service
- input interface

NetFlow switching operates by creating a flow cache that contains the information needed to switch and perform access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard switching path (fast or optimum). As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created, packets identified as belonging to an existing flow can be switched based on the cached information and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

## New Hardware Features in Release 11.1(12)CA1

The following new hardware features have been added to Release 11.1(12)CA1:

### High-Speed Serial Interface Port Adapters

The PA-H Revision B port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). This port adapter was revised to improve performance.

### E1-G.703/G.704 Serial Port Adapter

The E1-G.703/G.704 serial port adapters (PA-4E1G-120 and PA-4E1G-75) are available on Cisco 7500 series routers, Cisco 7200 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### JT2 6.3-MHz Serial Port Adapter

The JT2 6.3-MHz serial port adapter (PA-2JT2) is available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Hardware Features in Release 11.1(11)CA1

The following new hardware feature has been added to Release 11.1(11)CA1:

### PA-A2 ATM-CES Port Adapter

The PA-A2 ATM-CES port adapters (PA-A2-4T1C-OC3SM, PA-A2-4T1C-T3ATM, PA-A2-4E1XC-OC3SM, PA-A2-4E1XC-E3ATM, PA-A2-4E1YC-OC3SM, and PA-A2-4E1YC-E3ATM) are available on Cisco 7200 series routers.

## New Hardware Features in Release 11.1(10)CA

The following new hardware features have been added to Release 11.1(10)CA:

### Second-Generation Fast Ethernet Interface Processors

The second-generation Fast Ethernet Interface Processors (FEIP2-2TX and FEIP2-2FX) are available on Cisco 7500 series routers and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### Channelized E1 and T1 Port Adapters

The channelized E1 and T1 Primary Rate Interface (PRI) Integrated Services Digital Network (ISDN) port adapters (PA-2CE1/PRI-75, PA-2CE1/PRI-120, and PA-2CT1/PRI) are available on Cisco 7500 series routers and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Software Features in Release 11.1(10)CA

The following new software feature has been added to Release 11.1(10)CA:

### clock rate Command Enhancements

The **clock rate** command has been enhanced for the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). For these port adapters, the clock rate you enter is rounded (if needed) to the nearest value that your hardware can support.



**Note**

---

The enhancement to the **clock rate** command is also available in Cisco IOS Release 11.1(9)CA1.

---

## New Hardware Features in Release 11.1(9)CA1

The following new hardware features have been added to Release 11.1(9)CA1:

### Next-Generation Route Switch Processor (RSP4)

The RSP4 is available on Cisco 7500 series routers to provide improved performance.

### 100VG-AnyLAN Port Adapter

The 100VG-AnyLAN port adapter (PA-100VG) is available on Cisco 7200 series routers.

## PA-8B-ST and PA-4B-U Basic Rate Interface Port Adapters

The Basic Rate Interface (BRI) Integrated Services Digital Network (ISDN) port adapters (PA-8B-ST and PA-4B-U) are available on Cisco 7200 series routers.

## PA-2CE1/PRI-75, PA-2CE1/PRI-120, and PA-2CT1/PRI Channelized E1 and T1 Port Adapters

The channelized E1 and T1 Primary Rate Interface (PRI) Integrated Services Digital Network (ISDN) port adapters (PA-2CE1/PRI-75, PA-2CE1/PRI-120, and PA-2CT1/PRI) are available on Cisco 7200 series routers.

## Channelized T3 Interface Processor Feature Enhancements

The Channelized T3 Interface Processor (CT3IP) available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) now supports the following additional features:

- SNMP MIB support per RFC 1406 and RFC 1407
- Performance monitoring by Facility Data Link (FDL) in accordance with ANSI T1.403
- Remote FDL loopbacks
- Generation of bit error rate testing (BERT) patterns
- User-configurable yellow alarm processing

## PA-A1-OC3MM and PA-A1-OC3SMI ATM Port Adapters

The Asynchronous Transfer Mode (ATM) port adapters (PA-A1-OC3MM and PA-A1-OC3SMI) are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Hardware Features in Release 11.1(8)CA1

The following new hardware features have been added to Release 11.1(8)CA1:

### Packet OC-3 Interface Processor

The Packet OC-3 Interface Processor (POSIP) is available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### 100VG-AnyLAN Port Adapter

The 100VG AnyLAN port adapter (PA-100VG) is available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## PA-4R-FDX Token Ring Full-Duplex Port Adapter

The Token Ring full-duplex port adapter (PA-4R-FDX) is available on Cisco 7500 series routers, Cisco 7200 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## SA-Comp/1 and SA-Comp/4 Data Compression Service Adapters

Multiple SA-Comp/1 and SA-Comp/4 data Compression Service Adapters (CSAs) are available on Cisco 7200 series routers.

## New Software Features in Release 11.1(8)CA1

The following new software features have been added to Release 11.1(8)CA1:

### Fast-Switched Fragmented IP Packets

IP fast fragmentation is available on Cisco 7200 series routers.

### Fast-Switched SMRP Packets

Fast-switched Simple Multicast Routing Protocol (SMRP) is available on Cisco 7200 series routers.

### Particle-Based Transparent Bridging

Particle-based transparent bridging (TRB) is available on Cisco 7200 series routers.

### Source-Route Bridging Enhancements

Particle-based source-route bridging (SRB) is available on Cisco 7200 series routers.

### Turbo Flooding of UDP Datagrams

Turbo flooding of User Datagram Protocol (UDP) datagrams is available on Cisco 7200 series routers.

## New Hardware Features in Release 11.1(7)CA1

The following new hardware features have been added to Release 11.1(7)CA1:

### Channelized T3 Interface Processor

The Channelized T3 Interface Processor (CT3IP) is available on Cisco 7500 series routers and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### FDDI Full-Duplex Single-Mode and Multimode Port Adapters

The PA-F/FD-SM and PA-F/FD-MM FDDI full-duplex single-mode and multimode port adapters are available on Cisco 7200 series routers.

### Synchronous Serial Port Adapters

The PA-8T-X21 and PA-8T-232 synchronous serial port adapters are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Hardware Features in Release 11.1(6)CA

The following new hardware features have been added to Release 11.1(6)CA:

### FDDI Full-Duplex Single-Mode and Multimode Port Adapters

The PA-F/FD-SM and PA-F/FD-MM FDDI full-duplex single-mode and multimode port adapters are available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### High-Speed Serial Interface Port Adapters

The PA-H Revision B HSSI port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). Although the PA-H was introduced in Cisco IOS Release 11.1(6)CA, the minimum Cisco IOS release required by the PA-H is Release 11.1(12)CA or later or 11.2(7)P or later. For more information on the PA-H and PA-2H port adapters, refer to the *Field Notice: HSSI Port Adapters* publication on CCO at the following location:

<http://www.cisco.com/warp/customer/770/fn-pa-upgrade.shtml>

### Synchronous Serial Port Adapters

The PA-8T-V35 synchronous serial port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## SA-Comp/1 and SA-Comp/4 Data Compression Service Adapters

The SA-Comp/1 and SA-Comp/4 data Compression Service Adapters (CSA) are available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

## New Software Features in Release 11.1(6)CA

The following new software features have been added to Release 11.1(6)CA:

### High System Availability on a VIP

Release 11.1(6)CA also includes support for the high system availability (HSA) feature on a Versatile Interface Processor (VIP) or second-generation VIP (VIP2) in the Cisco 7500 series routers. For more information and important notes on HSA, refer to the *Release Notes for Cisco IOS Release 11.1*.

### RSP Optimum or Flow-Switched Fragmented IP Packets

IP fast fragmentation is available on Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

### Source-Route Bridging Enhancements

The following enhancements have been added to the Cisco 7200 series routers:

- Source route bridging (SRB) is now supported over Fiber Distributed Data Interface (FDDI).
- Particle-based switching is now supported for SRB packets (over FDDI and Token Ring) by default.

Particle-based switching adds scatter-gather capability to SRB to improve performance. Particles represent a communications data packet as a collection of noncontiguous buffers. The traditional Cisco IOS packet has a packet type control structure and a single contiguous data buffer. A particle packet has the same packet type control structure, but also maintains a queue of particle type structures, each of which manages its own block.

The scatter-gather architecture used by particle-based switching provides the following advantages:

- Allows drivers to use memory more efficiently (especially when using media that has a large maximum transmission unit [MTU]). For example, Token Ring buffers could be 512 bytes rather than 16 KB.
- Allows concurrent use of the same region of memory. For example, on IP multicast a single packet is received and sent out on multiple interfaces simultaneously. Allows insertion or deletion of memory at any location in a packet (not just at the beginning or end).

# MIBs

## Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-\* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 3](#).

**Table 3** *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

## Important Notes

The following sections contain important notes about Cisco IOS Release 11.1 CA and apply to Cisco 7000 family routers.

### Image Obsolescence, Cisco IOS Release 11.1(36)CA1

All Cisco 7200 series and Cisco 7500 series images in Cisco IOS Releases 11.1(36)CA have been obsoleted from manufacturing due to the following caveat:

- CSCds04747

These images are now available in Cisco IOS Release 11.1(36)CA1.

**Note**

---

Disclaimer: In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images. **PLEASE BE AWARE THAT FAILURE TO UPGRADE THE AFFECTED IOS IMAGES MAY RESULT IN NETWORK DOWNTIME.** The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

---

### End of Sales and End of Engineering for Cisco IOS Release 11.1 CA

When a Cisco IOS Software Release reaches End of Sales (EOS), it is no longer orderable. When a release reaches End of Engineering (EOE), no further maintenance releases are scheduled.

Cisco IOS Software Release 11.1 CA is scheduled to reach End of Sales with maintenance release 11.1(34)CA, and will no longer be orderable as of September 15, 2000. Note that release 11.1CA images will remain posted on CCO after EOS, though they will no longer be orderable with new systems. Release 11.1 CA will reach End of Engineering with maintenance release 11.1(36)CA3.

Until the declaration of General Deployment (GD) status for Cisco IOS Software Release 12.0, release 11.1CA was the preferred GD release on the Cisco 7200 and Cisco 7500 platforms. Cisco IOS Release 12.0 supports all features and hardware supported in release 11.1 CA, and is now the preferred GD release on these platforms. Customers requiring GD software are encouraged to migrate to release 12.0 after suitable review and acceptance testing.

For more information about the EoS and EoE of Cisco IOS Software Release 11.1 CA, refer to the Product Bulletin located on CCO at:

[http://www.cisco.com/warp/customer/cc/pd/rt/platform/prodlit/1122\\_pp.htm](http://www.cisco.com/warp/customer/cc/pd/rt/platform/prodlit/1122_pp.htm)

## Release 11.1(28)CA Command Modification

- CSCdm64565

When a router is configured with multiple interfaces configured with one or more Hot Standby Router Protocol (HSRP) groups, the **debug** command fails. A debug condition has been added to allow the output from the **standby debug** command to be filtered based upon interface and group number. The command utilizes the “debug condition” paradigm introduced into 12.0, and is of the form:

```
debug condition standby interface group
```

The interface must be a valid interface capable of supporting HSRP. The group may be any group (for example 0 to 255). A debug condition may be set for groups that do not exist. This allows debug to be captured during the initialization of a new group.

You must enable **standby debug** in order for any debug output to be produced. If no standby debug conditions exist, then debug output is produced for all groups on all interfaces. If at least one standby debug condition exists, then **standby debug** output is filtered according to all **standby debug** conditions.

## General Deployment Status

Release 11.1CA has achieved GD status based on extensive customer experience and use in diverse networks, analysis of stability and bug trends, and review of customer satisfaction surveys. Cisco Systems believes GD releases are, in general, suitable for unconstrained use in customers' networks for features and platforms supported in the release. In this case, GD status applies to maintenance releases 11.1(22)CA and later (within the 11.1CA release), and only on the Cisco 7200, 7500, and RSP7000-based 7000 platforms. For more information, refer to the Product Bulletin located at the following URL:

[http://www.cisco.com/warp/customer/cc/cisco/mkt/core/7500/prodlit/829\\_pb.htm](http://www.cisco.com/warp/customer/cc/cisco/mkt/core/7500/prodlit/829_pb.htm)

## Preferred Year 2000-Compliant Release

Release 11.1CA will be supported into the year 2000, and will remain orderable until Release 12.0 has reached GD status. Until that time, Cisco IOS Software Release 11.1CA GD for Cisco 7200 and 7500 is the preferred Year 2000-compliant GD release on Cisco 7200 and 7500 platforms. For more information, refer to the Product Bulletin located at the following URL:

[http://www.cisco.com/warp/customer/cc/cisco/mkt/core/7500/prodlit/829\\_pb.htm](http://www.cisco.com/warp/customer/cc/cisco/mkt/core/7500/prodlit/829_pb.htm)

## Release 11.1(20)CA1 Replaces 11.1(20)CA

Release 11.1(20)CA1 replaces 11.1(20)CA. Release 11.1(20)CA1 corrects the following caveats:

- CSCdk14917—The router reloads after net booting.
- CSCdk08256—The error message “SYS-2-BADSHARE: Bad refcount in datagram\_done” occurred on an ATM-CES card.
- CSCdk11218—When a PVC is congested, tunnel traffic leaks memory on the ATM CES port adapter.

- CSCdk28128—Transmit DMA might lock up on the VIP, with the PA-4R-DTR port adapter.
- CSCdk17982—The transmitter does not restart after the **no shutdown** command on the PA-4R-DTR port adapter.
- CSCdk21340—A PCI retry timeout occurs on the VIP2 with the PA-4R-DTR port adapter during Token Ring initialization.
- CSCdk19133—Two extra bytes are padded at the end of a TX frame if the end-of-frame bit is close to an underrun situation.
- CSCdk11997—The IP route-cache distributed feature is not working.
- CSCdj57131—The driver might issue the message “TokenRing3/2: Unexpected EXEC\_INT interrupt rcvd: code=0x7,” indicating that the MAC command interrupt processing is getting confused.
- CSCdk22861—The VIP2-50 does not support Token Ring or 100VG port adapters.
- CSCdk22195—New APPN subsystem object files are provided for the Release 11.1(20)CA build.
- CSCdk11985—Early token release causes the Token Ring interface to fail in full-duplex mode.

For additional information, refer to the *Field Notice: Cisco IOS Release 11.1(20)CA1* publication on CCO at the following location:

<http://www.cisco.com/warp/customer/770/>

## Release Schedule Changes

Cisco IOS Release 11.1 software has transitioned from a 7-week to a 13-week release model. To conform to that transition, some changes will occur in the Release 11.1 CA software schedule. Beginning with Release 11.1(18)CA, maintenance releases will deploy on a 13-week release cycle. For consistency with the former 7-week cycle, all maintenance releases will be built; however, only the even-numbered maintenance releases will be released. The odd-numbered maintenance releases, beginning with Release 11.1(19)CA, will not be released.

## Release 11.1(18)CA1 Replaces 11.1(18)CA

Release 11.1(18)CA1 replaces 11.1(18)CA. Release 11.1(18)CA1 corrects the following caveat:

- CSCdj93505—Processor memory parity checking does not work on the SDRAM-based VIP2-50 products or on any of the VIP2-10/15/20/40 products.

## Interoperability Guidelines for E3 and T3 Serial Port Adapters

Interoperability guidelines exist for E3 and T3 serial port adapter data service units. For interoperability guidelines for the E3 adapter, refer to the *E3 Serial Port Adapter Installation and Configuration* publication. For interoperability guidelines for the T3 adapter, refer to the *T3 Serial Port Adapter Installation and Configuration* publication. The documentation accompanies the hardware product and is also available on the Documentation CD-ROM and Cisco Connection Online (CCO).

## Recommended Software Release

This release note lists the Cisco IOS release in which a port adapter or interface processor was first announced. However, the minimum or recommended release of Cisco IOS software required for a port adapter or interface processor might be a later release. The recommended release changes periodically and might not be the same release in which the port adapter or interface processor was announced. In some cases, the change is to support new features and in other cases to correct caveats.

The hardware documentation that ships with the port adapter or interface processor lists the minimum release of Cisco IOS required to support the port adapter, which might not be the Cisco IOS you currently have running on your router. The hardware documentation is updated as often as possible to note changes in the Cisco IOS requirements. Manufacturing always ships the current minimum Cisco IOS release with the port adapter or interface processor. The latest Cisco IOS software is available on CCO.

## Release 11.1(14)CA1 Replaces 11.1(14)CA

Release 11.1(14)CA1 replaces 11.1(14)CA. Release 11.1(14)CA1 corrects the following caveats:

- CSCdj21539—Routers running remote source-route bridging (RSRB) from a Cisco 7200 or Cisco 7500 series router with a PA-4R Token Ring adapter insert an invalid Token Ring frame check sequence (FCS) in frames sent to remote peers. The invalid FCS causes data frames to be dropped on some remote peer routers. Affected remote peer routers are Cisco 2500 series, Cisco 4000 series, Cisco 4500 series, and Cisco 4700 series routers running Cisco IOS Release 10.2 or earlier. Other router models and routers running Cisco IOS Release 10.3 or later are not affected.
- CSCdj42431—A Cisco 7206 router restarts with a “CLSIMsgCreateFromPak” message after a crash dump on output from the **show stack** command.
- CSCdj44697—On a Cisco 7200 router under certain conditions, packets that saw an optimum cache miss and an input access list failure can cause another packet to be corrupted.
- CSCdj42984—When source-route bridging (SRB) is configured between two or more directly attached Token Ring interfaces in a router, Cisco IOS software recalculates and appends a new FCS (frame check sequence) cyclic redundancy check (CRC) to the end of the old FCS. This results in four extra bytes of “data” being added to the frame’s field.

For additional information, refer to the *Field Notice: Cisco 7200 IOS ED Release 11.1(14)CA Software Defects* document on CCO at the following location:

<http://www.cisco.com/warp/customer/770/35.shtml>

## Release 11.1(13a)CA1 Replaces 11.1(13)CA1

Release 11.1(13a)CA1 replaces 11.1(13)CA1. Release 11.1(13a)CA1 corrects the following caveat:

- CSCdj31496—Unpredictable failures occur in all routed protocols.

Workaround: To temporarily clear related routing problems, use the **clear ip route** command for IP. For all other protocols, use the **shutdown** command followed by the **no shutdown** command.

For additional information, refer to the *Field Notice: Cisco IOS Routed Protocol Defect* document on CCO at the following location:

<http://www.cisco.com/warp/customer/770/14.shtml>

## Release 11.1(13)CA1 Replaces 11.1(13)CA

Release 11.1(13)CA1 replaces 11.1(13)CA. Release 11.1(13)CA1 corrects the following caveat:

- CSCdj23465—The output from the **show stack** command might display configuration or password information obtained from the console buffer.

For additional information, refer to the *Field Notice: Cisco IOS Release 11.1(13)CA* document on CCO at the following location:

<http://www.cisco.com/warp/customer/770/13.shtml>

## Release 11.1(12)CA1 Replaces 11.1(12)CA

Release 11.1(12)CA1 replaces Release 11.1(12)CA. Release 11.1(12)CA1 corrects the following caveats:

- CSCdj23299—The CT3 reports massive overruns (up to 1100 per second) from the Route Switch processor (RSP) side. However, we later discovered that the overruns were not “real” overruns, but actually ignores being counted erroneously as overruns.
- CSCdj24098—Under heavy traffic conditions, the HSSI port adapter might handle packets abnormally. We strongly encourage customers using HSSI port adapters on Cisco 7200 series routers to upgrade to an image containing the fix for this bug.
- CSCdi64972—If a router is running out of memory while running Open Shortest Path First (OSPF). OSPF does not check to see if one of its structures has been properly allocated. This might result in a SegV exception and cause the router to reload.
- CSCdj24890—The internal clock of the ATM port adapter is not initialized properly. This defect causes a loopback ping to fail because neither end is providing a clock.
- CSCdj18696—The IEEE spanning tree Bridge Protocol Data Units (BPDUs) are not recognized by a VIP2 with a PA-4R in Cisco IOS Release 11.1(10)CA or 11.1(11a).
- CSCdj04220—When the **debug atm event** command is enabled on an ATM port adapter, the driver generates a spurious memory access while it tries to fetch statistics for all VCs.
- CSCdj24569—The OutPkts and InBytes per VC statistics counter shown by the **show atm vc** command is incorrect.

## Release 11.1(11)CA1 Replaces 11.1(11)CA

Release 11.1(11)CA1 replaces 11.1(11)CA. Release 11.1(11)CA1 corrects caveat CSCdj17858 for Cisco 7200 series images—when an INARP VC is configured on an ATM port adapter while the interface is in a shutdown state, after the interface is brought up, the ATM port adapter might cause the router to reload the next time an INARP packet is received.

## Recommended Upgrade to Release 11.1(10)CA

To eliminate several problems associated with the VIP2, POSIP, and CT3IP products, we recommend that you upgrade to Cisco Release 11.1(10)CA or later. For more information on these problems and for other recommended Cisco IOS software versions, refer to the *Field Notice: VIP2 Cisco IOS Software Release Deferrals* publication posted on Cisco Connection Online (CCO) at the URL listed below. CCO is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

<http://www.cisco.com/warp/customer/770/6.shtml>

## Release 11.1(9)CA1 Replaces 11.1(9)CA

Release 11.1(9)CA1 replaces Release 11.1(9)CA. Release 11.1(9)CA1 resolves caveat CSCdi89690—on PA-H and PA-2H HSSI port adapters, users might experience CRC, overrun, and underrun when a second HSSI port adapter is installed and running on the same VIP2. For information on this caveat, see the “[Resolved Caveats—Release 11.1\(9\)CA1](#)” section on page 52.

## Release 11.1(8)CA1 Replaces 11.1(8)CA

Release 11.1(8)CA1 replaces Release 11.1(8)CA. Release 11.1(8)CA1 corrects MIP and POSIP microcode versions and corrects the ROM monitor version required for the RSP4.

## Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 11.1 and Cisco IOS Release 11.1 CA are also in Cisco IOS Release 11.1(36)CA3.

For information on caveats in Cisco IOS Release 11.1, see *Release Notes for Cisco IOS Release 11.1* on CCO and the Documentation CD-ROM. These release notes contain caveats affecting all maintenance releases and list severity 1 and 2 caveats for Cisco IOS 11.1 CA1.



### Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

**Table 4** Caveats Reference for 11.1 CA

DDTS Number	Software Release	
	11.1 CA	
	Caveat Corrected	Caveat
CSCdi64972	X	
CSCdi80889	X	
CSCdi85841	X	
CSCdi89690	X	
CSCdj00388	X	
CSCdj02254	X	
CSCdj02702	X	
CSCdj03646	X	
CSCdj04220	X	
CSCdj04555	X	
CSCdj05999	X	
CSCdj08350	X	
CSCdj08510	X	
CSCdj11905	X	
CSCdj12822	X	
CSCdj12951	X	
CSCdj13110	X	
CSCdj13405	X	
CSCdj13409	X	
CSCdj15129	X	
CSCdj15134	X	
CSCdj16922	X	
CSCdj16985	X	
CSCdj17314	X	
CSCdj18441	X	
CSCdj18684	X	
CSCdj18685	X	
CSCdj18696	X	
CSCdj19970	X	
CSCdj19977	X	
CSCdj21320	X	
CSCdj21539	X	
CSCdj23299	X	
CSCdj23465	X	

Table 4 Caveats Reference for 11.1 CA (continued)

DDTS Number	Software Release	
	11.1 CA	
	Caveat Corrected	Caveat
CSCdj24098	X	
CSCdj24283	X	
CSCdj24479	X	
CSCdj24569	X	
CSCdj24584	X	
CSCdj24890	X	
CSCdj25270	X	
CSCdj26196	X	
CSCdj29751	X	
CSCdj31158	X	
CSCdj31496	X	
CSCdj31863		X
CSCdj37556	X	
CSCdj37583	X	
CSCdj41153	X	
CSCdj42431	X	
CSCdj42984	X	
CSCdj44697	X	
CSCdj45833	X	
CSCdj45966	X	
CSCdj46388	X	
CSCdj46564	X	
CSCdj50587	X	
CSCdj51644	X	
CSCdj51914	X	
CSCdj54192	X	
CSCdj54728	X	
CSCdj55839	X	
CSCdj57131	X	
CSCdj59745	X	
CSCdj60813	X	
CSCdj62406	X	
CSCdj63149	X	
CSCdj63926	X	

**Table 4** Caveats Reference for 11.1 CA (continued)

DDTS Number	Software Release	
	11.1 CA	
	Caveat Corrected	Caveat
CSCdj64103	X	
CSCdj64479	X	
CSCdj66230	X	
CSCdj67478	X	
CSCdj69502	X	
CSCdj70353	X	
CSCdj71335	X	
CSCdj74820	X	
CSCdj76260	X	
CSCdj83870	X	
CSCdj86581	X	
CSCdj87212	X	
CSCdj88756	X	
CSCdj89025	X	
CSCdj90253	X	
CSCdj90469	X	
CSCdj93505	X	
CSCdj94991	X	
CSCdk07175	X	
CSCdk07546	X	
CSCdk08256	X	
CSCdk08868	X	
CSCdk10762	X	
CSCdk11218	X	
CSCdk11985	X	
CSCdk11997	X	
CSCdk14917	X	
CSCdk17982	X	
CSCdk18176	X	
CSCdk19133	X	
CSCdk19469	X	
CSCdk21340	X	
CSCdk22030	X	
CSCdk22195	X	

Table 4 Caveats Reference for 11.1 CA (continued)

DDTS Number	Software Release	
	11.1 CA	
	Caveat Corrected	Caveat
CSCdk22861	X	
CSCdk22991	X	
CSCdk23479	X	
CSCdk25825	X	
CSCdk27388	X	
CSCdk28128	X	
CSCdk32125	X	
CSCdk34128	X	
CSCdk35028	X	
CSCdk39193	X	
CSCdk39920	X	
CSCdk39936	X	
CSCdk41217	X	
CSCdk42813	X	
CSCdk42931	X	
CSCdk44597	X	
CSCdk50505	X	
CSCdk62872	X	
CSCdk63484	X	
CSCdk65504	X	
CSCdk69969	X	
CSCdk67709	X	
CSCdk69452		X
CSCdk74431	X	
CSCdk78652	X	
CSCdk79774	X	
CSCdm00163	X	
CSCdm10910	X	
CSCdm13956	X	
CSCdm18715	X	
CSCdm20942	X	
CSCdm38825	X	
CSCdm46683	X	
CSCdm46735	X	

**Table 4** Caveats Reference for 11.1 CA (continued)

DDTS Number	Software Release	
	11.1 CA	
	Caveat Corrected	Caveat
CSCdm57609	X	
CSCdm64501	X	
CSCdm64565	X	
CSCdm69594	X	
CSCdm71714	X	
CSCdm78351	X	
CSCdp15392	X	
CSCdp25457	X	
CSCdp32279	X	
CSCdr27894	X	
CSCdr87607	X	
CSCds04747	X	
CSCdw65903	X	

## Open Caveats—Cisco IOS Release 11.1(36)CA3

This section documents possible unexpected behavior by Cisco IOS Release 11.1(36)CA3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 11.1(36)CA3.

## Resolved Caveats—Cisco IOS Release 11.1(36)CA3

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CA3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw78210

Related to fixes in CSCdw65903 and outlined in:

<http://www.cisco.com/warp/public/707/cisco-malformed-snmplib-pub.shtml>.

This defect may be seen when “debug snmp packets” is turned on and can result in tracebacks.

## Open Caveats—Cisco IOS Release 11.1(36)CA2

This section documents possible unexpected behavior by Cisco IOS Release 11.1(36)CA2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 11.1(36)CA2.

## Resolved Caveats—Cisco IOS Release 11.1(36)CA2

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CA2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

## Open Caveats—Release 11.1(36)CA1

This section documents possible unexpected behavior by Cisco IOS Release 11.1(36)CA1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

### Basic System Services

- CSCdk69452

Regular expression matching in an RSP2 or RSP4 with Border Gateway Protocol (BGP) configured may enter into an infinite loop when an as-path statement containing a pipe [|] regular expression character is used. This infinite loop may cause the router to reload. There is no workaround.

### TCP/IP Host-Mode Services

- CSCdj31863

A Cisco router running Cisco IOS Release 11.1CA may reload under certain rare circumstances when running remote shell (rsh) service. This happens under certain unknown circumstances when some remote system connects to the router using UNIX-style RSH commands.

Workaround: Disable RSH service by using the **no ip rcmd rsh-enable** command.

## Resolved Caveats—Release 11.1(1) Through 11.1(36)CA

This section describes possibly unexpected behavior by Release 11.1(36)CA and describes only severity 1 and 2 caveats:

### IP Routing Protocols

- CSCdp25457

A Cisco 7500 series router may lose some routing entries even though all routers in the network have the correct EIGRP topology and neighboring routers contain all routing entries with successors.

Workaround: Issue the **clear ip eigrp neighbor** command.

## Miscellaneous

- CSCds04747

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at

<http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

## Resolved Caveats—Release 11.1(1) Through 11.1(36)CA

This section describes possibly unexpected behavior by Release 11.1(36)CA and describes only severity 1 and 2 caveats:

### IP Routing Protocols

- CSCdm64501

A Cisco 7000 series router running either inbound or outbound access lists may cause IP fast packets to process switch instead of fast switch. Without access lists the packets are switched as expected. There is no workaround.

### Basic System Services

- CSCdk23479

Large configurations (larger than 128K) cannot be saved to the Flash memory card with a **write memory** command when the CONFIG\_FILE variable is set to a file in Flash memory.

Workaround: Use the **copy running slot0:filename** command. Configurations can also be saved to NVRAM with the **service compress-configuration** command.

## Wide-Area Networking

- CSCdr87607

When you load system software to upgrade from any version of the following Cisco IOS releases: 11.1 CC, 11.1 CA, 11.2 P, or 12.0 to any Cisco IOS Release 12.1 or later, the system logging messages for Frame Relay DLCI and subinterface status change are suppressed, regardless of the logging destination (console, buffer, or host).

Workaround: To resume generating Frame Relay DLCI logging messages, issue the **logging event dlci command**. To resume generating subinterface status messages, issue the **logging event subif** command.

## Resolved Caveats—Release 11.1(1) Through 11.1(34)CA

This section describes possibly unexpected behavior by Release 11.1(34)CA and describes only severity 1 and 2 caveats:

### Interfaces and Bridging

- CSCdm18715

When a Cisco router is configured with the **bandwidth 250000** configuration command under the X.25 serial interface, the following error message appears:

```
%RSP-3-RESTART: interface Serial4/4, output stuck
```

Next, the Cisco router is continuously looped and the console is flooded with messages about the interfaces going up and down. The following message keeps appearing in the loops:

```
%RSP-3-RESTART: cbus complex
```

You must power cycle the Cisco router to stabilize it.

Workaround: Do not use the **bandwidth** configuration command with the X.25 serial interface.

### IP Routing Protocols

- CSCdm78351

A Cisco router has a valid EIGRP metric for a route but does not update neighboring EIGRP routers, which show the route as inaccessible and keep it out of the routing table.

Workaround: Issue the **clear ip eigrp neighbor** command for each neighbor that does not have the route in its routing table.

- CSCdr27894

A Cisco 7500 series router may reload when a **show ip route** command is entered due to a missing memory lock on rdb during printing.

Workaround: Do not use the **show ip route** command.

## Resolved Caveats—Release 11.1(1) Through 11.1(32)CA

This section describes possibly unexpected behavior by Release 11.1(32)CA and describes only severity 1 and 2 caveats:

### Interfaces and Bridging

- CSCdk41217

When under a traffic load, a Cisco 7206 router with an FDDI interface goes administratively down when another Cisco 7206 router is inserted into the FDDI ring. The problem is also indicated with the following syslog messages:

```
Aug 30 08:42:24 abc01 72: Aug 30 12:45:07: %FDDI-3-FDDIFAIL: interface fddi0Duplicate
MAC address detected , , = 0x0 Aug 30 08:43:15 abc01 85: Aug 30 12:45:57:
%FDDI-3-FDDIFAIL: Interface fddi0Duplicate MAC address detected , , = 0x0 Aug 30
08:43:15 def01 34777: Aug 30 12:45:57: %FDDI-3-FDDIFAIL: Interface fddi0Duplicate MAC
address detected , , = 0x0 Aug 30 10:38:18 def01 69: Aug 30 14:41:01:
%FDDI-3-FDDIFAIL: Interface fddi0Duplicate MAC address detected , , = 0x0.
```

There is no workaround.

- CSCdp15392

A PA-4R-DTR port adapter or a Cisco 2600 series router sometimes inserts at the wrong ring speed. The interface recognizes the incorrect ring speed and removes itself from the ring. If the router is connected to a Smart controlled access unit (CAU), the Smart CAU might disable the port because of the incorrect ring speed. In this situation, the router will try to re-insert into the ring, but it will not be able to. This condition is rare and will not cause any physical problems with the ring. Unless the router is connected to a Smart CAU, which will wrap the port automatically, this condition is difficult to detect. There is no workaround.

### Miscellaneous

- CSCdm69594

The interface delay metric is set incorrectly for port channel interfaces where one or more Gigabit Ethernet interfaces are grouped into a channel. The delay for a single Gigabit Ethernet interface is 10 microseconds. The delay for a port channel made up of one or more Gigabit Ethernets is 100 microseconds. The incorrect setting might seriously impact routing protocols that use interface delay as part of the metric (for example, Enhanced Interior Gateway Routing Protocol (EIGRP)), and might cause the routing protocol to take a route through a single interface over a route through a port channel.

Workaround: Manually configure an appropriate delay under the port channel interface by entering the **delay** *tens of microseconds* interface configuration command.

## Resolved Caveats—Release 11.1(1) Through 11.1(30)CA

All caveats listed in this section are resolved in Cisco IOS Release 11.1(30)CA. This section describes only severity 1 and 2 caveats:

### Basic System Services

- CSCdp32279

When a Cisco 7500 series router running Cisco IOS Release 11.1(29)CA is used as a tftp server, the **copy tftp flash** command fails. There is no workaround.

### ISO CLNS

- CSCdj18685

A reboot is caused by an AVL node that is freed but is still accessed during tree traversing. This problem is a result of the node being deleted and freed in the middle of a tree walk. This is a problem specific to Intermediate System-to-Intermediate System (IS-IS) (using an AVL tree). There is no workaround.

### Wide-Area Networking

- CSCdm46683

A Cisco 7500 series router with a VIP card may not respond to an RSP board request for a DBus transaction. The RSP finds the DBus internal error bit set in a VIP status register and does a CBus complex restart, displaying the following error messages:

```
%DBUS-3-DBUSINTERR: Slot x, Internal Error
%RSP-3-RESTART: cbus complex
```

Workaround: Enter, and then exit the if-consoles of each VIP in the router.

## Resolved Caveats—Release 11.1(1) Through 11.1(28)CA

All the caveats listed in this section are resolved in Release 11.1(30)CA. This section only describes severity 1 and 2 caveats:

### Basic System Services

- CSCdj83870

A Cisco Discovery Protocol (CDP) device will generate an alignment error when doing a Simple Network Management Protocol (SNMP) walk if one of the devices in its neighbor cache table does not have an assigned network address.

Workaround: Assign all CDP neighbor devices with a network address.

## Interfaces and Bridging

- CSCdj54192

If an interface on an HSSI 1 port (PA-H or H1T+) card goes down and you see the following error message, you may be experiencing this bug:

```
%MUSELIX-1-STOPFAIL: XXXX: Stop Failed at disable port (XXXX = the interface affected)
%MUSELIX-1-STARTFAIL: XXXX: Start Failed at enable port MUESLIX-1-FAILURE_CAUSE:
SerialX/X:
```

This condition is caused by several factors.

Workaround: Once the interface is in this state, issue the following test commands where <CR> is a carriage return:

```
term len 0<CR> sh cont h 1/0<CR> test tpu b<CR> 1/0<CR> g<CR> x<CR> y<CR> r<CR>
s<CR> 3<CR> q<CR> test tpu b<CR> 1/1<CR> g<CR> x<CR> y<CR> r<CR> s<CR>
3<CR> q<CR> test len 24<CR>
```

- CSCdm38825

Source-route bridging using a PA-4R-DTR token ring card may result in frames occasionally being bridged out of order. For protocols that are sensitive to the sequence order of frames, such as LLC2, intermittent session loss may occur. There is no workaround.

- CSCdm46735

A PA-4R-DTR port may reset under the following circumstances:

- A high rate of traffic is traversing the port (200 pps or better).
- The PA-4R-DTR port is the Active monitor of the physical ring.
- An event on the ring occurs that forces the active monitor to purge the ring.

When this problem occurs, the PA-4R-DTR port will reset, and the ring will experience a beacon.

Workaround: Make sure the PA-4R-DTR port is not the active monitor on the ring. This can be done by ensuring that the MAC-address of the DTR card is not the highest MAC-address on the physical ring.

- CSCdm71714

A PA-2CT1 does not display information about throughput if Fancy Queueing is enabled.

Workaround: Disable Fancy Queueing.

## IBM Connectivity

- CSCdm20942

A Cisco 7000 series router might reload with a bus error when you change the STUN (serial tunnel) protocol group that an active STUN interface belongs to.

Workaround: Make sure the STUN interface is shut down before changing the STUN group.

## IP Routing Protocols

- CSCdk08868  
The Lock and Key idle timers are taking too long to time out. The idle timeout, as configured by the **autocommand access-enable** command, is taking too long to time out. When the logging is on for access list hits, the time that it takes to idle out (with no access list hits) takes up to two times the length configured.  
  
If the dynamic entry created by the Lock and Key feature requires the user to telnet into the router, then the idle timeout will take up to two times the length configured by using the **autocommand access-enable host timeout *minutes*** command.  
  
Workaround: Upgrade to Cisco IOS Release 11.2 if this problem occurs while running Cisco IOS Release 11.1 images.
- CSCdm13956  
Internet Control Message Protocol (ICMP) redirects can overwhelm process switching on a router and consume all available memory.  
  
Workaround: Issue a **clear ip redirect** command or reload the router.

## Miscellaneous

- CSCdj67478  
After an interface is removed using online insertion and removal (OIR), the ARP entries associated with the interface may not be removed from the ARP table.  
  
Workaround: Issue the **clear arp** command after the OIR to remove the entries.
- CSCdk78652  
The PA-A2 driver might free itself twice for aborted transmitted packets or particles. This might occur when you change shaping parameters or shut down the router while active traffic is going through the port adapter. There is no workaround.
- CSCdm57609  
A PA-A2 port adapter might cause memory corruption if you use switched virtual circuits (SVCs) with an address resolution protocol (ARP) server when you shut down the interface. There is no workaround.

## TCP/IP Host-Mode Services

- CSCdm00163  
A Cisco 7500 router running Cisco IOS Release 11.1(20)CA reloads due to a bus error pointing at a null pointer (0x0). The following error message is displayed:  
  

```
System restarted by bus error at PC 0x27BD0060, address 0x0
```

  
This problem happens under rare unknown conditions when multiple Telnet sessions are run from the router.  
  
Workaround: Upgrade to Cisco IOS Release 12.0 or use a later release of Cisco IOS Release 11.1CA, such as 11.1(26.02)CA, or do not run the Telnet sessions from the router.

## Resolved Caveats—Release 11.1(26)CA

All the caveats listed in this section are resolved in Release 11.1(28)CA. This section only describes severity 1 and 2 caveats:

### Basic System Services

- CSCdk63484

In certain circumstances, the IPX Enhanced Interior Gateway Routing Protocol (EIGRP) topology table and the routing table do not show entries for routes that are showing on other IPX EIGRP neighbors. The affected Cisco router does show that the updates are being received when DEBUG IPX EIGRP is used, but the entries are never added to the topology table. There is no workaround.

### Interfaces and Bridging

- CSCdj41153

In Cisco 7500 series routers, it is possible to get an RSP-2-QAERROR that results from the duplication of a packet pointer, resulting in a CBus complex restart. There is no workaround.

- CSCdk42931

A Cisco 7513 router running the Release 11.1(20)CA1 Enterprise feature set with a Fast Ethernet Interface Processor (FEIP) fails to bridge Maintenance Operation Protocol (MOP) load request packets (destination MAC ab00.0010.0000) when the receiving Fast Ethernet interface is configured for bridging and more than ten active Hot Standby Router Protocol (HSRP) groups.

Workaround: Replace the FEIP with a Fast Ethernet port adapter and a VIP card if it is on a Cisco 7500 series platform. Another workaround is to reduce the total number of HSRP groups on one interface by moving some HSRP groups to another interface.

- CSCdk67709

Multilink PPP interleaving causes delays in outbound traffic on RSP platforms. There is no workaround.

- CSCdm10910

When any of the interfaces on a loaded Cisco 7513 router on the Fast Serial Interface Processor in slot 9 are enabled (**no shutdown**), the router reloads. There is no workaround.

### IP Routing Protocols

- CSCdk22030

This scalability issue occurs when established peers time out during high activity after you use the **clear ip bgp** command or after a reload. As a result, it takes longer for all the Border Gateway Protocol peers to converge. The **clear ip bgp** command should be avoided. There is no workaround.

### Miscellaneous

- CSCdk65504

While using distributed Cisco Express Forwarding (dCEF), the interface output counters fail to update and the VIP console displays the error message FIB-4-FIBXDRLLEN. This caveat is found in Release 11.1(21)CC2 and 11.1(22)CC. There is no workaround.

## Resolved Caveats—Release 11.1(24)CA

All the caveats listed in this section are resolved in Release 11.1(26)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdk79774

Under heavy load conditions, a Cisco 7000 family router with VIP-based PA-4R, PA-4R-FDX, or PA-4R-DTR Token Ring interfaces may forward packets containing four extra bytes. The four bytes are appended to the end of the packet. This may adversely affect protocols sensitive to frame lengths (that is, IBM SNA sessions may fail). There is no workaround.

## Resolved Caveats—Release 11.1(22)CA

All the caveats listed in this section are resolved in Release 11.1(24)CA or later. This section only describes severity 1 and 2 caveats:

### Basic System Services

- CSCdk32125

When the router is running low on memory and a **write memory** or **configure network** command is issued, the NVRAM may be corrupted and the router may reload.

Workaround: Check whether there is enough memory to write the configuration.

- CSCdk27388

Packet fragmentation can bring down the VIP by causing the DMA engine to stall. There is no workaround.

### DECnet

- CSCdj63149

DECnet data packets going out on the dialer interface do not cause the link to come up if the router has been configured with DECnet static routes pointing to that interface.

Workaround:

- For intra-area traffic, use the command:  
**dialer-list 1 protocol decnet\_router-l1 permit** (assuming a group number of 1)
- For inter-area traffic, use the command:  
**dialer-list 1 protocol decnet\_router-l2 permit**

## Interfaces and Bridging

- CSCdk19469

If a single-attached PA-FDDI goes down because of a problem on the FDDI ring, the PA-Fast Ethernet may begin logging “output stuck” syslog messages and stop passing traffic to the Fast Ethernet interface.

Workaround: Clear the FDDI interface or use the **shutdown/no shutdown** commands. Then both the FDDI and the Fast Ethernet interfaces resume normal operation. Another workaround is to replace the PA-FDDI with an FDDI interface processor.

- CSCdk07175

Interfaces on the CT1 failed to forward packets.

Workaround: Issue the **shutdown/no shutdown** commands on the primary rate interface to have packets begin forwarding again.

- CSCdk35028

Three Fast Ethernets configured for full-duplex will not work.

Workaround: Configure one Ethernet for full-duplex, and the other two for half-duplex. Another workaround is to configure all three interfaces for half-duplex.

- CSCdk74431

A large packet sent over a Multilink PPP (MLP) bundle (greater than two links) with VPDN on an ATM PPP tunnel on an ATM-Lite interface can become corrupted.

Workaround: Disable fast switching on the ATM-Lite interface.

## IP Routing Protocols

- CSCdk66969

With synchronization and certain topologies, some BGP routes may not get advertised after peer reset.

Workaround: Configure **no synchronization** or **clear ip bgp x.x.x.x** commands.

## Miscellaneous

- CSCdk50505

Cisco 7000 series and 7500 series routers running Release 11.2(15) with an ATM Interface Processor connection to an LS1010, RFC1483 SVC configuration might reload because of memory corruption caused by the User-Network Interface (UNI) 3.1 Service Specific Connection Oriented Protocol (SSCOP) retransmission path. This is caused if the ATM signal to the LS1010 is lost.

Workaround: Configure UNI 3.0 in the ATM interfaces.

- CSCdk62872

Segmentation and reassembly (SAR) does not see the line pressure properly and swamps the multiplexing device chip, which causes cell drops for both UBR and CBR. There is no workaround.

## Wide-Area Networking

- CSCdk42813

When multicast fast switching is run, small packets coming from a LANE subinterface that need to be routed to another LANE subinterface are not sent correctly. Runts appear on the Ethernet interfaces connected to a Catalyst 5000. There is no workaround.

## Resolved Caveats—Release 11.1(20)CA

All the caveats listed in this section are resolved in Release 11.1(22)CA or later. This section only describes severity 1 and 2 caveats.

### Basic System Services

- CSCdk22991

If the total size of a Frame Relay compressed packet grows in the output queue, a buffer in an internal data structure can be misqueued and cause the router to reload. There is no workaround.

### Interfaces and Bridging

- CSCdj94991

When running Release 11.1CA, the VIP can reload with a software-forced reload, giving a traceback pointing to `vip_pak_to_host_inline`. This has been seen with a VIP2-based Packet OC-3 Interface Processor (POSIP), although it potentially can occur with other interfaces. The problem has only been seen on two occasions in the last three months.

Workaround: Recover the RSP by doing a microcode reload.

- CSCdk10762

After a reload or CBus complex restart, there is a small chance (one in several thousand) that one or more T1 lines in a CT3IP does not come back up properly.

The symptoms are that the line comes up correctly at both ends. There are no T1 alarms or performance monitoring errors detected and the line protocol is down (assuming keepalives are enabled). The far-end router counts large numbers of CRC errors in its relevant **show interface** counters. The near-end router (the relevant CT3IP interface) does not show any errors in its counters. The T1 number is 1–20 (T1s 21–28 are not affected by this problem).

Workaround: Reload the microcode or reload the router.

All Cisco IOS releases that support CT3IP have recently been modified to include more details in the hardware version string displayed in the output of the **show controllers t3** command.

Prior to firmware version 2.8.0, this display only showed a hardware version of 5, as seen in this example:

```
Router# show controllers t3 0/0/0
T3 0/0/0 is up. CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.7.0
```

After upgrading to a Cisco IOS image that includes firmware version 2.8.0 or later, the above display will be enhanced to include more hardware version details, as seen in these two examples:

```
Router# show controllers t3
T3 0/0/0 is up. CT3 H/W Version: 5.0.0, CT3 ROM Version: 1.2, CT3 F/W Version: 2.8.0
```

```
Router# show controllers t3 T3
0/0/0 is up. CT3 H/W Version: 5.0.1, CT3 ROM Version: 1.2, CT3 F/W Version: 2.8.0
```

Hardware versions 5.0.0 and 5.0.255 are subject to this caveat. Hardware version 5.0.1 is not.

Workaround: If you see a hardware version of 5 with no additional numbers, update your software to a more recent version.

- CSCdk18176

After booting Release 11.1(18.1)CA with bridging enabled on the ATM interface (AIP), the Cisco 7513 router with an RSP4 continuously reboots with a bus error. When bridging is removed from the ATM interface, the router stays up. It also causes the router at the other end of the PVC to reload with a software-forced reboot. This was also experienced with Release 11.1(18)CA.

Workaround: Bridge on ATM using Release 11.1(14)CA.

- CSCdk39193

HSSI 3 code waits for a chip reset at the beginning of the code. However, a chip reset is done only at booting after online insertion and removal. This problem did not show up earlier because when both TX/RX clocks are present, bit 0 of STATUS6 is also set, so the microcode can proceed with no problem. However when there is only one clock, the microcode sticks at PC=0.

Workaround: Proceed regardless of the reset status, as the old HSSI microcode did.

- CSCdk39936

An FEC that uses Fast Ethernet port adapters in full-duplex mode needs this fix. Caveat CSCdk20683 caused this condition. Any release that has CSCdk20683—11.1(21)CA, 11.1(21)CC, 12.0(0.17)—exhibits this condition in which line states of FEC members keep toggling.

Workaround: Upgrade your images to Release 11.1(22)CA, 11.1(22)CC, or 12.0(0.22).

- CSCdk44597

The PA-A1 ATM port adapter cannot transmit Operation, Administration, and Maintenance (OAM) cells. There is no workaround.

## LLC Type 2

- CSCdk07546

Frames retransmitted by an Advanced Peer-to-Peer Networking (APPN) router using remote source-route bridging (RSRB) are truncated. There is no workaround.

## Miscellaneous

- CSCdk34128

When the router generates sufficient network traffic to saturate a serial interface on an M4T or M8T adapter, it can result in packet memory becoming depleted. The only way to recover the memory is to reload the router. There is no workaround.

## Wide-Area Networking

- CSCdk25825  
When Enhanced Online Insertions Removal (EOIR) hot swapping is performed from one type of ATM card to another, the **show lane xxx** command might display incorrect LANE information. This does not affect LANE connectivity. There is no workaround.
- CSCdk39920  
When packets are bridged while a VC is torn down, an incorrect VC value (zero) might be recorded in the bridge table entry. As a result, packets are dropped. This occurs because the VC value is set to zero before the subinterface is brought down.  
Workaround: Remove the invalid bridge entry by executing the **clear bridge** command.

## Resolved Caveats—Release 11.1(18)CA

All the caveats listed in this section are resolved in Release 11.1(20)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj63926  
The console on Cisco 7500 series HSA systems might become unresponsive with configurations larger than 128K and service compress configured. The console can lock up when a **write memory** or **copy running** command is issued, and the configuration NVRAM can become corrupted and inaccessible. Other VTYS and packet forwarding and routing operations continue unimpeded while the console or Telnet EXEC is nonresponsive.

Workaround: Store the configuration in Flash memory. For example, use the following commands:

```
copy running slot0:config
boot config slot0:config
service compress
boot buffersize N
```

where *N* is at least three times the configuration size in bytes. Then the **write memory** command works slowly. Expect 10 minutes elapsed time for each 128K block of configuration text.

Use the following procedure to recover configuration NVRAM after it is corrupted:

- Send an RS-232 break to the console of both master and slave.
- Use the ROM monitor **config-register** command on both master and slave to ignore system configuration.
- Use the ROM monitor **reset** command on both master and slave and boot a slave-capable image.
- On the master console, copy the correct configuration file from Flash memory or TFTP into the running configuration file.
- Turn off the 0x40 bit in the configuration register by using the **show version EXEC** command and the **config-register** configuration command.
- Reload the master.

- CSCdj88756

To allow Web traffic to be redirected selectively to Web caches by the Web Cache Control Protocol (WCCP) feature, access list support was added. This feature was added to eliminate the use of the source IP address by some Web servers as an authentication mechanism. (The Web cache currently acts as a proxy and uses its own address as the source for requests.)

The following command was added at the global configuration level:

```
ip wccp redirect-list acl
```

In Release 11.1 CA, *acl* is a number from 1 to 199 used to reference an IP access list (standard or extended). For software release 11.2 P, *acl* can be any number from 1 to 199 or a named IP access list (standard or extended).

The output for the **show ip wccp** command was modified to give feedback about how the access list support is performing:

```
router# show ip wccp
Global WCCP information:
Number of web-caches:2
Total Packets Redirected:101
Redirect access-list:no_linux
Total Packets Denied Redirect:88
Total Packets Unassigned:0
```

There is no workaround

- CSCdj89025

A Cisco 7200 series router connected by serial ports to a synchronous serial port adapter (PA-8T) might experience interface resets.

There is no workaround.

- CSCdj90469

On Cisco 7200 series routers, poor compression performance is obtained when you use the **frame-relay payload-compress packet-by-packet** command. There is no workaround.

- CSCdj87212

A Cisco 7206 router with an FDDI and PA-A1 ATM port adapter (LANE) interface can pause indefinitely when configured with transbridging between the ATM and FDDI interfaces. There is no workaround.

- CSCdj66230

The ATM interface in the VIP reloaded because of memory block corruption. There is no workaround.

- CSCdj86581

For synchronous serial port adapters (PA-4T+) the **transmitter-delay** command might not be enabled. There is no workaround.

- CSCdj90253

For VIP/PA-4R and VIP/PA-4R-FDX Token Ring interfaces configured for source-route bridging (SRB), automatic spanning tree can begin cycling endlessly between the “up” and “initializing” states.

Workaround: Configure manual SRB spanning tree.

- CSCdj64479

Under rare conditions, EIGRP might not converge after a route flap. There is no workaround.

- CSCdj70353

A Cisco 7000 series Route Switch Processor (RSP7000) reloads when Frame Relay encapsulation is enabled on the High-Speed Serial Interface (HSSI).

Workaround: Disable fast switching.

- CSCdj15129

On rare occasions after the router powers up, after the router is reloaded, or after the microcode is reloaded, the PA-2CT1/PRI port adapter on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) might stop transmitting data because of a framer lockup condition.

To verify that the interface is functioning properly after a system power-up, system reload, or microcode reload, a successful **ping** command must be confirmed across the interface. If the ping fails and the line and protocol are up, it might indicate a framer lockup condition. To verify that a framer lockup condition exists, disable keepalives on the interface for the duration of the test. After disabling keepalives, wait about 40 seconds, use the **ping** command, and use the **show interface** command to check the line and protocol status. If the **ping** command fails, and the line and protocol are up after disabling keepalives, a framer lockup condition exists.

Workaround: Reload the microcode and then check the status of the interface (with the procedure above). If the condition still exists, you must reload the router and check the status of the interface again. To fully release this condition if a reload of the microcode and router are not sufficient, you must power cycle the router.

- CSCdj15134

On rare occasions after the router powers up, after the router is reloaded, or after the microcode is reloaded, the PA-2CE1/PRI port adapter on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) might exhibit CRC errors on all receive-side packets. These packets are subsequently dropped by the port adapter.

To verify that the interface is functioning properly after a system power-up, system reload, or microcode reload, a successful **ping** command must be confirmed across the interface. A ping that fails when the line and protocol are up, might indicate this CRC error condition. To verify that this CRC error condition exists, disable keepalives on the interface for the duration of the test. After disabling keepalives, wait about 40 seconds, use the **ping** command, and use the **show interface** command to check the line and protocol status. If the **ping** command fails, and the line and protocol are up after disabling keepalives, this CRC error condition exists.

Workaround: Reload the microcode and then check the status of the interface (with the procedure above). If the condition still exists, you must reload the router and check the status of the interface again. To fully release this condition if a reload of the microcode and router are not sufficient, you must power cycle the router.

## Resolved Caveats—Release 11.1(17)CA

All the caveats listed in this section are resolved in Release 11.1(18)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj76260

After source-route bridging is configured on FDDI, many ignored packets are visible on a Cisco 7500 series router with the VIP2 FDDI port adapter. Older Fiber Distributed Data Interface (FIP) cards do not show the ignored packets.

Workaround: Use a FIP card.

- CSCdj69502

When channelized E1 port adapters and weighted fair queueing are configured, all interfaces of the channelized E1 port adapters have many dropped packets.

Workaround: Configure the following on each interface:

```
no fair-queue
no ip route-cache distributed
transmit-buffers backing-store
```

- CSCdj71335

File transfers between a Token Ring host and another host connected through Fast EtherChannel can cause CPU utilization to increase between 80% to 100%. This increase occurs in both directions. The same operation works correctly when the Token Ring-attached host is accessed through another media type, such as ATM.

Workaround: Disable Fast EtherChannel.

- CSCdj74820

When Fast EtherChannel is configured on a Cisco 7500 series router, the following error messages are displayed:

```
%RSP-3-ERROR: CyBus1 error 10
%CBUS-3-CMDTIMEOUT: Cmd timed out
%RSP-3-RESTART: cbus complex
```

Workaround: Disable distributed fast switching (DFS).

- CSCdj54728

EIGRP might cause the router to reload when it receives updates in a network that has a major topology change in conjunction with a large EIGRP topology database. There is no workaround.

- CSCdj62406

The **distribute-list in** command does not filter static or summary (null0) routes. There is no workaround.

- CSCdj12951

Better crash information is needed to debug data or stack corruption reloads. The solution is to write reload information to default to bootflash:reloadinfo in the RSP and flash:reloadinfo in the RP. A series of **test crash** command selections is used to control and change the crashinfo collection mechanism. The crash information contains up to 32 KB in the RSP and up to 20 KB in the RP of errmsg log plus command history, including configuration commands that the user enters. The crash information also contains up to 32 KB on the RSP and 20 KB on the RP for all the following information:

- Crash stack trace
- Crash context
- Stack dump at crash
- Dump memory for each register containing “valid” RAM address
- Errmsg display on invalid length of bcopy
- Two commands to “test crash”

The **show stack** command displays (“cat” as in UNIX) the bootflash:crashinfo file if there was a crash. The user can also use the **copy flash tftp** command to dump the ASCII file bootflash/flash:crashinfo to a server.

The size is 16 KB of errmsg and command information plus up to 16 KB of memory dump and other crash information. There is one 16-KB DRAM declared for this crash information collection mechanism.

Only Cisco 7000 series routers and the RSP are supplied with the new crashinfo mechanism and the 16 KB. The Cisco 4500 router and others see no difference. There is no workaround.

## Resolved Caveats—Release 11.1(16)CA

All the caveats listed in this section are resolved in Release 11.1(17)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj59745

The RSP reloads at `rsp_fs_free_memd_pack`. This might be caused by older versions of ATM Interface Processor (AIP) microcode in the router that is reloading or in routers that are supplying this router in the same network. There is no workaround.

- CSCdj51644

A situation occurs with bridging between LANE and FDDI where a Cisco router does not handle packets appropriately. There is no workaround.

- CSCdj60813

With serial links on VIP port adapters, users experience incrementing interface resets and serial line flaps under heavy load.

Workaround: Turn off fair queueing.

- CSCdj64103

Under rare circumstances, a router with BGP enabled sees BGP updates with a duplicate community attribute, which triggers the neighbor to reset. There is no workaround.

- CSCdj55839  
With certain route map configurations or soft reconfigurations, the localpref for a path might be set to 0, resulting in the wrong path being selected. There is no workaround.
- CSCdj04555  
On a Fast Serial Interface Processor (FSIP) four- or eight-port card when you are running at clock rates greater than 4 Mbps, you might see overruns or underruns. The serial controllers on the FSIP are limited to 6.132 Mbps each. The four-port FSIP has one serial controller, and the eight-port FSIP has two, one for ports 0–3 and one for ports 4–7. When one or more ports consume the entire 6.132 Mbps bandwidth, you need to administratively shut down the other ports on the serial controller. If you exceed the 6.132-Mbps limitation, underruns or overruns are expected. There is no workaround.

## Resolved Caveats—Release 11.1(15)CA

All the caveats listed in this section are resolved in Release 11.1(16)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj37556  
A Cisco 7200 series or Cisco 3600 series router might reload with a bus error when performing a protocol translation between X.25 and PPP.  
Workaround: Enable header-compression passive in the translate statement.
- CSCdj50587  
Channelized E1 port adapters (PA-2CE1) that are configured as ISDN PRI in a Cisco 7500 series router can quickly run out of transmit queue (txq) credits and lock up, especially if call turnover is high. To remove this lock-up condition and restore the port adapter functionality, reload the router.  
The problem can be seen with the **show controllers cbus** command, issued when the port adapters are in a deadlock condition. To see if credits have been lost, issue a **show controllers cbus** command several times. If credits are lost, the txacc value should never go back to txlimit. Eventually, all credits are depleted, and the controller ceases to function.  
Additional indicators are that ISDN Layer 2, as seen with the **show isdn status** command, remains in the TEI-ASSIGNED state. Also, you might see an “output hang” message when you issue the **show interface** command for the D channel. There is no workaround.
- CSCdj24283  
A VIP interface card on an RSP router might see a reload under some unusual circumstances. If you encounter this problem, the symbols resulting from decoding the EPC in the output of the **show diag** command output show emulate\_load\_store. There is no workaround.
- CSCdj26196  
Consecutive rapid Packet over SONET (POS) interface transitions might cause the VIP to reload at configsonetplx(0x60112454)+0x110. There is no workaround.
- CSCdj45833  
When BGP dampening is on, a withdraw and announce combination for a route is counted as two flaps. A flap should not be counted when a withdrawn route is reannounced. There is no workaround.
- CSCdj46564  
A VIP2 card with a Token Ring port adapter installed reloads and resets the interface.  
Workaround: Rebooting sometimes helps to recover.

- CSCdj51914

A Cisco 7206 router reloads when the channel service unit (CSU) is powered off. There is a connection through ATM to an ISP doing ATM to Frame Relay to the CSU that connects to a Cisco 2500 router. If the CSU is powered down within 1 to 2 minutes, the Cisco 7206 reloads with a bus error. There is no workaround.

- CSCdj45966

With a large number of subnets, a CPUHOG message like the following might be generated:

```
7000 running 11.0.16 getting:
.Sep 30 17:55:32:%SYS-3-CPUHOG: Task ran for 2608 msec (73/65), Process = BGP
scanner, PC = 176388
```

There is no workaround.

## Resolved Caveats—Release 11.1(14)CA

All the caveats listed in this section are resolved in Release 11.1(15)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj46388

The display from a **show controllers** command on a PA-2E3 port adapter in a Cisco 7500 series or Cisco 7200 series router might inaccurately report the hardware revision number of the port adapter. A Cisco 7200 series router might report “Version 2” with the **show controllers serial** command. A Cisco 7500 series router might report “HW Revision 0x2” with the **show controllers serial** or **show controllers cbus** commands. Hardware revision 3 is the first available revision number for this port adapter.

Workaround: Look at the board itself for the hardware revision number.

- CSCdj31158

The no buffer counter on the ATM interface of the ATM-CES port adapter for Cisco 7200 series routers does not increment correctly. It spuriously records a no buffer condition even if hardware buffers are available. There is no workaround.

- CSCdj19977

Memory fragmentation can result if many “radixmnodetypes” are “mallored/freed” by Cisco IOS software in a short period.

Workaround: Upgrade to larger DRAM modules (128 MB), especially for ISP sites.

- CSCdj37583

When the OSPF interface **ip ospf authentication-key** *key* command is configured with a key length that is longer than 19 characters (including any trailing spaces), the OSPF internal data is corrupted and a following **write terminal** or **show running-config** command could reload the router. Also, this problem might occur with the **ip ospf message-digest** *key-id* **md5** *key* command if the key length is longer than 36 characters.

Workaround: Do not enter a key longer than 19 characters (or 36 characters for the **ip ospf message-digest** command), whether encrypted or not.

- CSCdj05999 CSCdj17314

A defect in “ip\_cache\_ager” was found at a customer site under abnormal conditions where both ends of a high-speed point-to-point link were configured with the same IP address. This is not expected to occur in more normal circumstances, nor have we been successful in recreating this problem in the laboratory.

Workaround: Do not configure the same IP address on both ends of a high-speed link.

- CSCdj12822 CSCdi80889

The Cisco 7206 brings serial interfaces down as soon as the fourth T1 line is enabled on the router. After the fourth line is connected, the lines remain up for approximately 15 minutes and then display the following message:

```
%OIR-3-SEATED: Insert/removal failed (slot 4), check card seating.
```

There is no workaround.

## Resolved Caveats—Release 11.1(13a)CA1

The caveats listed in this section are resolved in Release 11.1(14)CA or later. This section only describes severity 1 and 2 caveats.

- CSCdj02702

When you run IP multicast over LAN Emulation (LANE) on the ATM port adapter, there is a possibility that the ATM port adapter will receive cell FIFO overrun. This subsequently causes related input packets to be dropped. This condition has been observed when the IP multicast traffic reaches a certain rate.

Workaround: Although this problem is negligible when the source traffic is shaped at a lower rate, we recommend that IP multicast over LANE not be used until the cause of the problem is found and a fix is determined.

- CSCdj03646

A Cisco 7200 series router with an eight-port serial adapter might pause indefinitely and display the following error messages:

```
%SYS-2-INLIST: Buffer in list
%Link-2-NOSOURCE: source idb not set.
```

Workaround: Reload the router.

- CSCdj21320

A VIP2 with an HSSI and Fast Ethernet port adapter reloads because of a memory corruption. The console shows the following messages:

```
%VIP2x-1-MSG,
%DBUS-3-DBUSINTERR,
%RSP-3-RESTART,
%RSP-3-FOREVER []
```

There is no workaround.

- CSCdj24584

When a new E1 line is added, the PA-8T might enter an unstable up-down situation. This instability might cause the VIP2-20 to reload. There is no workaround.

- CSCdj25270

The ATM port adapter on Cisco 7500 series routers might experience call setup failures and display the following messages:

```
AIPREJCMD
AIP-3-FAILCREATEVC
```

There is no workaround.

- CSCdj29751

In RSP-based platforms, the following error might occur that indicates a problem with a hardware enqueue:

```
%RSP-2-QAERROR: reused or zero link error, write at addr 00C0 (QA) log 2600C040, data
00070000 00000000."
```

This might be followed by the following error:

```
"Unexpected exception, CPU signal 10, PC = 0x601C4658"
```

The router might reload. This problem is caused by a bad memory access in the diagnostic code handling the original QA error. There is no workaround.

- CSCdj24479

The VIP2 FDDI port adapter transparently bridges traffic even though there is no bridge group defined on the interface.

Workaround: Use the **no bridge-group 1** command on the FDDI port adapter interface.

- CSCdj08350

A spurious memory access can occur when switching from flow switching to process switching using the **no ip route-cache** command and then back to flow switching using the **ip route-cache flow** command. There is no workaround.

- CSCdj18684

The register dump provides valuable information that helps to determine the root cause of a reload, especially those caused by memory corruption. This fix enhances the register dump and crashinfo in general by:

- Providing not only the deallocator of a freed block but also the previous deallocator
- Providing better early memory corruption detection when “debug sanity” is on
- Detecting whether the data in a register is inside a malloc block; if so, the entire malloc block (up to 1 KB) is dumped
- Checking the contents of the register memory dump for valid RAM addresses and dumping them as well (this is useful for dump places such as pak->datagramstart or hwidb->next)
- Consolidating all memory dumps into up to 96 dump blocks to eliminate duplicate dumps on the same or nearby areas

## Resolved Caveats—Release 11.1(12)CA1

All the caveats listed in this section are resolved in Release 11.1(13a)CA1 or later. This section only describes severity 1 and 2 caveats:

- CSCdj13405
 

When asymmetrical compression algorithms are configured (that is, **compress stac** on one router and **compress predictor** on another), both routers can crash or lock up. The migration to Stac from predictor causes this problem.

Workaround: Shut down the interfaces, change compression algorithms on both ends, and then start up or use the **no shutdown** command on the interface.
- CSCdj13409
 

The VIP PA-4R port adapter is bridging frames that were aborted by the sender rather than dropping the aborted frames. There is no workaround.
- CSCdj18696
 

IEEE spanning tree bridge protocol data units are not recognized by a VIP2 with an NP-4R running Cisco IOS Release 11.1(10)CA or 11.1(11). There is no workaround.
- CSCdj08510
 

An encapsulation change on a POS interface can result in a PCI timeout VIP reload. This results from the POS interface accessing onboard registers before the onboard PLX chips are programmed. There is no workaround.
- CSCdj11905
 

When an FDDI ring is highly unstable and is having excessive transitions, the FDDI interface might go down.

Workaround: Use the **clear interface** command.
- CSCdj18441
 

Under high traffic conditions, the HSSI port adapter might handle packets abnormally. Customers using VIP2/HSSI port adapters are strongly encouraged to upgrade to an image containing the fix for this bug. See the *Field Alert: VIP2 Cisco IOS Software Release Deferrals* publication for image availability and additional information.
- CSCdj16985
 

If one person is doing a **write memory** command and another person does a **show configuration** command at the same time, the router might reload. There is no workaround.
- CSCdj16922
 

The **show ip bgp neigh x.x.x.x adv** command with route-map deny community does not work. There is no workaround.
- CSCdj19970
 

With certain traffic, NetFlow switching can cause a loss of MEMD buffers, causing the interface to pause indefinitely. There is no workaround.

## Resolved Caveats—Release 11.1(11)CA1

The caveats listed in this section are resolved in Release 11.1(12)CA1 or later. This section only describes severity 1 and 2 caveats.

- CSCdj13110

Under stress conditions, when you remove or insert an interface processor card in a powered-up router that contains a VIP2 with an ATM port adapter (PA-A1-OC3MM or PA-A1-OC3SMI), the ATM port adapter reloads. During the reload period, the ATM interface is down and cannot transmit or receive packets.

Workaround: Do not remove or insert an interface processor card in a powered-up router that contains a VIP2 with an ATM port adapter.

## Resolved Caveats—Release 11.1(10)CA

All the caveats listed in this section are resolved in Release 11.1(11)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdj00388

Multiring IP/IPX does not function on FDDI interfaces in Cisco 7500 series routers. There is no workaround.

## Resolved Caveats—Release 11.1(9)CA1

All the caveats listed in this section are resolved in Release 11.1(10)CA or later. This section only describes severity 1 and 2 caveats:

- CSCdi85841

Multiring IP/IPX does not function in Cisco 7200 series routers. There is no workaround.

- CSCdj02254

Users might experience FDDI interface Output Stuck errors when running FDDI port adapters along with other high-bandwidth port adapters (for example, Fast Ethernet) in the same VIP under very high VIP aggregate bit-rate loads. When this error occurs, the FDDI interface is reset and resumes operation.

Workaround: Use the FDDI port adapter without a second port adapter in the VIP (that is, the other port adapter slot on the VIP must be empty).

A fix for this problem has been integrated in the hardware. We recommend that you replace the FDDI port adapter. For more information on CSCdj02254, refer to the *Field Notice: FDDI Port Adapter Replacement Recommendation* posted on Cisco Connection Online (CCO) at the URL:

<http://www.cisco.com/warp/customer/770/fna-isp.shtml>

## Resolved Caveats—Release 11.1(9)CA

All the caveats listed in this section are resolved in Release 11.1(9)CA1 or later. This section only describes severity 1 and 2 caveats:

- CSCdi89690

On PA-H and PA-2H HSSI port adapters, users might experience CRC, overrun, and underrun errors when a second HSSI port adapter is installed and running on the same VIP2. “Overrun” refers to a condition in which the HSSI port adapter sends more data to the VIP2 buffer than the buffer is capable of storing and forwarding. The HSSI port adapter does not have the capacity to reduce the amount of traffic it is sending. Data lost in this overrun condition is measured in packets lost. “Underrun” might occur when data from the VIP2 is sent to the buffer in the HSSI port adapter for transmission over the serial network. Under bidirectional load, the HSSI port adapter might fail to fetch data fast enough on transmit. Underruns are registered when this occurs.

Workaround: Use only one port on a PA-2H. VIP firmware is currently under test to remedy this problem. There is no other workaround.

Release 11.1(9)CA1 has fixes that alleviate CSCdi89690 but do not completely resolve the problem. For more information on CSCdi89690, refer to the *Field Notice: Cisco IOS Software Release 11.1(9)CA1* posted on Cisco Connection Online (CCO) at the following URL:

<http://www.cisco.com/warp/customer/770/fa1119CA1-2.html>

## Related Documentation

The following sections describe the documentation available for the Cisco 7000 family of routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 54](#)
- [Platform-Specific Documents, page 54](#)
- [Feature Modules, page 55](#)
- [Cisco IOS Software Documentation Set, page 55](#)

## Release-Specific Documents

The following documents are specific to Release 11.1 and are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 11.1*

On CCO at:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1: Release Notes: Cross-Platform Release Notes**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1: Release Notes: Cross-Platform Release Notes**

On Cisco.com at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes: Caveats**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Caveats**



### Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Cisco IOS Bug Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools>.

## Platform-Specific Documents

These documents are available for the Cisco 7000 family routers on CCO and the Documentation CD-ROM.

On CCO at:

**Technical Documents: Documentation Home Page: Cisco Product Documentation: Core/High-End Routers**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Core/High-End Routers**

## Feature Modules

Feature modules describe new features supported by Release 11.1 CA and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1 CA and Feature Modules**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1 CA and Feature Modules**

## Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

## Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Configuration Guides and Command References**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Configuration Guides and Command References**

## Cisco IOS Release 11.1 Documentation Set Contents

Table 5 lists the contents of the Cisco IOS Release 11.1 software documentation set, which is available in electronic form and also in printed form if ordered.



**Note**

You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

You can reach the Cisco IOS documentation set from CCO at:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1**

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1**

**Table 5 Cisco IOS Release 11.1 Documentation Set**

<b>Books</b>	<b>Major Topics</b>
<ul style="list-style-type: none"> <li><i>Configuration Fundamentals Configuration Guide</i></li> <li><i>Configuration Fundamentals Command Reference</i></li> </ul>	Access Server and Router Product Overview Understanding the User Interfaces Loading Images and Configuration Files Configuring Interfaces System Management
<ul style="list-style-type: none"> <li><i>Network Protocols Configuration Guide, Part 1</i></li> <li><i>Network Protocols Command Reference, Part 1</i></li> </ul>	AppleTalk IP Routing Protocols Novell IPX
<ul style="list-style-type: none"> <li><i>Network Protocols Configuration Guide, Part 2</i></li> <li><i>Network Protocols Command Reference, Part 2</i></li> </ul>	Apollo Domain Banyan VINES DECNet ISO CLNS

**Table 5** Cisco IOS Release 11.1 Documentation Set (continued)

<b>Books</b>	<b>Major Topics</b>
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	Wide-Area Networking Overview ATM Frame Relay ISDN SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point Support SNA Frame Relay Access Support APPN IBM Channel Attach
<ul style="list-style-type: none"> <li>• <i>Configuration Guide Master Index</i></li> <li>• <i>Command Reference Master Index</i></li> </ul>	

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
 Document Resource Connection  
 170 West Tasman Drive  
 San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

# Open Source License Acknowledgements

The following notices pertain to this software license.

## OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 53.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

Copyright © 1999–2002, Cisco Systems, Inc.  
All rights reserved.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].