



Release Notes for Cisco 7000 Family for Cisco IOS Release 11.1 CC

June 19, 2003

Cisco IOS Release 11.1(36)CC7

78-5116-19 E0

These release notes for Cisco 7000 family of routers describe the enhancements provided in Cisco IOS Release 11.1 CC, up to and including Cisco IOS Release 11.1(36)CC7. These release notes are updated as needed.

Use these release notes in conjunction with the *Release Notes for Cisco IOS Release 11.1* and *Release Notes for Cisco 7000 Family for Cisco IOS Release 11.1 CA*, located on CCO and on the Documentation CD-ROM. All features supported in Release 11.1 and Release 11.1 CA are supported in Release 11.1 CC.

For a list of the software caveats that apply to Cisco IOS Release 11.1CC, see the [“Caveats” section on page 29](#). The software caveats that apply to Cisco IOS Release 11.1 and Release 11.1 CA also apply to Release 11.1 CC. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and on the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 7](#)
- [MIBs, page 22](#)
- [Important Notes, page 23](#)
- [Caveats, page 29](#)
- [Related Documentation, page 71](#)



- [Obtaining Documentation, page 75](#)
- [Obtaining Technical Assistance, page 76](#)
- [Open Source License Acknowledgements, page 78](#)

Introduction

Cisco IOS Release 11.1(17)CC was the first release of this platform-specific Cisco IOS software. Cisco IOS Release 11.1(17)CC is available on Cisco Connection Online (CCO) only and cannot be ordered through manufacturing. Cisco IOS Release 11.1(18)CC or later is available on CCO and can be ordered through manufacturing. CCO is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services. For more information on Cisco IOS Release 11.1 CC, see *Cisco IOS Software Release 11.1 CC New Features* product bulletin #727, *Cisco IOS Software Release 11.1 CC Ordering Procedures and Platform Hardware Support* product bulletin #728, and *Cisco IOS Software Release Process for Release 11.1 CC* product bulletin #754 located on CCO.

Cisco Systems provides several software releases based on a single version of Cisco IOS software. Release 11.1 is a major release, and Cisco IOS Release 11.1(17) is a maintenance release. Maintenance releases deliver fixes to software defects only, thus providing the most stable software for your network and the features you need. In addition to the major release, there are several early deployment (ED) releases. The ED release, Cisco IOS Release 11.1 CC, delivers fixes to software defects and support for the new features of the Cisco 7000 family. For more information, see *Types of Cisco IOS Software Release Process* product bulletin #537 located on CCO.

Detailed software configuration information on the new features and Cisco IOS commands supported by Cisco IOS Release 11.1 CC are available on the Documentation CD-ROM and on the Web at <http://www.cisco.com>. For more information, see the [“Related Documentation” section on page 71](#). This document will be updated as additional releases of Cisco IOS Release 11.1 CC are made available to support new hardware and software features.

System Requirements

This section describes the system requirements for Cisco IOS Release 11.1(36)CC5 and includes the following sections:

- [Memory Recommendations, page 3](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 5](#)
- [Microcode, page 6](#)
- [Feature Set Tables, page 6](#)

Memory Recommendations

[Table 1](#) describes the memory recommendations for the feature sets for the Cisco 7000 family supported by Cisco IOS Release 11.1 CC. The following list contains additional important information for Cisco IOS Release 11.1 CC:

- Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the RSP7000 and RSP7000CI are shipped with a 16- or 20-MB Flash memory card.
- The Cisco 7200 series boot image has been changed to a self-decompressing compressed image, because the uncompressed boot image exceeds 4 MB.
- For port adapter hardware and memory configuration guidelines for the Cisco 7200 series routers, see the document *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines*.
- If you configure CEF or dCEF on Cisco 7500 series routers, use the following minimum memory requirements.
 - A configuration with fewer than 10,000 routes requires a minimum of 32 MB on the RSP and 16 MB on the VIP2-20.
 - A configuration with fewer than 20,000 routes requires a minimum of 64 MB on the RSP and 16 MB on the VIP2-20.
 - A configuration with more than 20,000 routes requires a minimum of 128 MB for the RSP and 32 MB on the VIP2-40.

For more information, see the Cisco Express Forwarding feature module.

Table 1 Memory Recommendations for the Cisco 7000 Family

Platforms	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	Enterprise	c7200-j-mz	8 MB Flash	32 MB DRAM	RAM
	Enterprise Plus APPN	c7200-aj-mz	8 MB Flash	32 MB DRAM	RAM
	Desktop Plus 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
Cisco RSP 7000/7500	Enterprise with VIP	rsp-jv-mz	16 MB Flash	32 MB DRAM	RAM
	Enterprise Plus APPN with VIP	rsp-ajv-mz	16 MB Flash	32 MB DRAM	RAM

Supported Hardware

Cisco IOS Release 11.1 CC supports the following platforms:

- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI)

[Table 2](#) summarizes the LAN interfaces supported on the Cisco 7000 family of routers.

[Table 3](#) summarizes the WAN data rates and interfaces supported on the Cisco 7000 family of routers.

Tables 2 and 3 use the following conventions:

- Yes—The particular data rate or interface is supported.
- No—The particular data rate or interface is not supported.

All port adapters and interfaces supported in Cisco IOS Release 11.1 CA are supported in Cisco IOS Release 11.1 CC.

For detailed descriptions of the new hardware features, see the [“New and Changed Information” section on page 7](#).

Table 2 LAN Interfaces Supported for the Cisco 7000 Family

Interface	Cisco 7200 Series	Cisco 7500 Series and Cisco 7000 Series with RSP7000
Ethernet (AUI)	Yes	Yes
Ethernet (10BaseT)	Yes	Yes
Ethernet (10BaseFL)	Yes	Yes
Fast Ethernet (100BaseTX)	Yes	Yes
Fast Ethernet (100BaseFX)	Yes	Yes
Token Ring 4-Mbps	Yes	Yes
Token Ring 16-Mbps	Yes	Yes
Token Ring full-duplex	Yes	Yes
FDDI DAS	Yes	Yes
FDDI SAS	No	Yes
FDDI full-duplex	Yes	Yes
FDDI multimode	Yes	Yes
FDDI single-mode	Yes	Yes
ATM interface	Yes	Yes
Channel interface	No	Yes
Second-generation channel interface	No	Yes
Parallel Channel Adapter (bus and tag)	No	Yes
ESCON Channel Adapter (ECA)	No	Yes
Versatile interface	No	Yes
Second-generation versatile interface	No	Yes
Multichannel interface (Channelized E1/T1)	Yes	Yes
100VG-AnyLAN	Yes	Yes

Table 3 WAN Data Rates and Interfaces Supported for the Cisco 7000 Family

Data Rates or Interface	Cisco 7200 Series	Cisco 7500 Series and Cisco 7000 Series with RSP7000
Data Rate		
48/56/64 kbps	Yes	Yes
1.544/2.048 Mbps	Yes	Yes
34/45/52 Mbps	Yes	Yes
Interface		
EIA/TIA-232	Yes	Yes
X.21	Yes	Yes
V.35	Yes	Yes
EIA/TIA-449	Yes	Yes
EIA-530	Yes	Yes
EIA/TIA-613 (HSSI)	Yes	Yes
ISDN BRI	Yes	No
ISDN PRI	Yes	Yes
E1-G.703/G.704	Yes	Yes
Channelized T1 and E1	Yes	Yes
Channelized T3 and E3	Yes	Yes
Packet-over-SONET OC-3 Interface	Yes	Yes
Serial	Yes	Yes
Enhanced ATM T3, E3, and OC3	Yes	Yes
ATM CES T3, E3, OC3, and T1/E1	Yes	No

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family, 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)CC5,
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 4](#) lists the current microcode versions for the Cisco 7000 family.

Table 4 Current Microcode Versions for the Cisco 7000 Family

Processor or Module	Current Bundled Route Switch Processor Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	10.12
EIP (Ethernet Interface Processor)	20.6	10.1
FEIP (Fast Ethernet Interface Processor)	20.8	10.2
FIP (FDDI Interface Processor)	20.4	10.2
FSIP (Fast Serial Interface Processor)	20.9	10.12
HIP (HSSI Interface Processor)	20.2	10.2
MIP (MultiChannel Interface Processor)	22.3	11.4
POSIP (Packet OC-3 Interface Processor)	20.1	20.1
TRIP (Token Ring Interface Processor)	20.2	10.3
VIP/VIP2 (Versatile Interface Processor/ second-generation Versatile Interface Processor 2)	21.40	21.9

Feature Set Tables

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.

Cisco IOS Release 11.1(36)CC5 supports the same feature sets as Cisco IOS Release 11.1 CC.

For information on these features, see *Release Notes for Cisco IOS Release 11.1*.



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.



Note

All features in Cisco IOS Release 11.1 CC are in all feature sets.

[Table 5](#) lists the feature sets supported by Cisco 7000 series, Cisco 7200 series and Cisco 7500 series routers in Cisco IOS Release 11.1(36)CC5.

**Note**

This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 11.1(36)CC5 by using the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 5 Feature Sets Supported by the Cisco 7000 Family

Feature Sets	Image Names	Feature Set Matrix Term	Software Image	Platforms
Enterprise Standard Feature Set	Enterprise	Basic ¹	c7200-j-mz	Cisco 7200
	Enterprise VIP	Plus ²	rsp-jv-mz	Cisco RSP7000/7500
Enterprise/APPN Standard Feature Set	Enterprise/APPN	Basic	c7200-aj-mz	Cisco 7200
	Enterprise/APPN/VIP	Plus	rsp-ajv-mz	Cisco RSP7000/7500
Desktop/IBM Standard Feature Set	Desktop/IBM	Basic	c7200-dr-mz	Cisco 7200
Network Layer 3 Switching Standard Feature Set	Network Layer 3 Switching	Basic	c7200-inu-mz	Cisco 7200

1. This feature set is offered in the Basic feature set.
2. This feature set is offered in the Plus feature set.

New and Changed Information

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

New Features in Cisco IOS Release 11.1(36)CC5

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)CC5.

New Features in Cisco IOS Release 11.1(36)CC4

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)CC4.

New Features in Cisco IOS Release 11.1(36)CC2

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)CC2.

New Features in Cisco IOS Release 11.1(36)CC1

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)CC1.

New Features in Cisco IOS Release 11.1(36)CC

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)CC.

New Features in Cisco IOS Release 11.1(35)CC

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(35)CC.

New Features in Cisco IOS Release 11.1(34)CC

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)CC.

New Features in Cisco IOS Release 11.1(33)CC1

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(33)CC1.

New Features in Cisco IOS Release 11.1(33)CC

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(33)CC.

New Features in Cisco IOS Release 11.1(32)CC

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)CC.

New Features in Cisco IOS Release 11.1(31)CC

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(31)CC.

New Features in Cisco IOS Release 11.1(30)CC

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)CC.

New Features in Cisco IOS Release 11.1(29)CC

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(29)CC.

New Features in Cisco IOS Release 11.1(28)CC

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)CC.

New Features in Cisco IOS Release 11.1(27)CC

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(27)CC.

New Features in Cisco IOS Release 11.1(26)CC

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)CC.

New Features in Cisco IOS Release 11.1(25)CC

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(25)CC.

New Features in Cisco IOS Release 11.1(24)CC

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)CC.

New Features in Cisco IOS Release 11.1(23)CC

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(23)CC.

New Features in Cisco IOS Release 11.1(22)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(22)CC supports the following new features:

PA-MC-T3 Multi-Channel T3 Port Adapter

The PA-MC-T3 Multi-Channel T3 port adapter is now available on the Cisco 7200 series routers.

The PA-MC-T3 port adapter provides one T3 interface connection through BNC connectors and transmits and receives data bidirectionally at the T3 rate of 44.736 Mbps. The interface provides up to 28 T1 lines (a single T3 group). Each T1 line is presented to the system as a serial interface that can be configured individually.

For more information on the PA-MC-T3 port adapter, refer to the *PA-MC-T3 Multi-Channel T3 Port Adapter Installation and Configuration* publication that accompanies the hardware.

Gigabit Ethernet Interface Processor

The Gigabit Ethernet Interface Processor (GEIP) is available on all Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI. The GEIP is a single-port fixed configuration interface processor that, when combined with the appropriate optical fiber cable, provides one 1000-Mbps IEEE 802.03-compliant Gigabit Ethernet interface. The Gigabit Ethernet interface operates in full-duplex mode at 1000 Mbps in each direction: transmit (TX) and receive (RX).

For more information on the Gigabit Ethernet Interface Processor, refer to the *Gigabit Ethernet Interface Processor (GEIP) Installation and Configuration* publication that accompanies the hardware.

New Minimum Cisco IOS Release for PA-A3

The current revision of a key component used in the Enhanced ATM Port Adapter (PA-A3) for Cisco 7500 series and Cisco 7200 series routers is being discontinued and replaced with a new revision by the manufacturer.

This new revision does not add or remove any hardware features from the PA-A3, and it is transparent to the PA-A3 functionality in Cisco 7500 series and Cisco 7200 series routers. However, the manufacturer did make minor internal changes to the component that have required Cisco to add software microcode to the PA-A3 port adapter.

To address the component revision change, Cisco IOS Release 11.1(22)CC (orderable as 11.1[22]R) is the new minimum Cisco IOS release required for the Enhanced ATM Port Adapter (PA-A3). Cisco IOS Release 11.1(22)CC is required for all new PA-A3 port adapter deployments in Cisco 7500 series and Cisco 7200 series routers.

**Note**

Although existing PA-A3 port adapters continue to function properly on releases prior to Cisco IOS Release 11.1(22)CC, Cisco requires that PA-A3 port adapters in the field be upgraded to Cisco IOS Release 11.1(22)CC as soon as possible.

This upgrade will ensure that all PA-A3 port adapters deployed will operate on a consistent Cisco IOS release. Furthermore, this upgrade will ensure that no issues arise from adding new PA-A3 port adapters to an existing network, because of network growth or through replacement port adapters.

Cisco 7576 Router

The Cisco 7576 router is the newest member of the Cisco 7500 series routers. It supports multiprotocol, multimedia routing, and bridging with a wide variety of protocols and any combination of available electrical interfaces and media.

The Cisco 7576 router consists of two independent routers configured on a single backplane. This system is housed within the chassis footprint of a Cisco 7513 router. The dual independent router design effectively doubles the system bandwidth that exists in the Cisco 7513 router.

Network interfaces reside on interface processors that provide a direct connection between the two independent dual CyBuses located on the backplane of the Cisco 7576 and your external network. The two independent dual CyBuses facilitate the configuration of two independent routers on a single backplane.

There are bays for up to two AC-input or DC-input power supplies. The Cisco 7576 can operate with only one power supply. Although a second power supply is not required, it allows load sharing and increased system availability.

For additional information, see the *Cisco 7576 Installation and Configuration Guide*.

Limited ATM OAM Management

The ATM operation, administration, and maintenance (OAM) management capabilities allow the state of point-to-point subinterfaces to be changed as a result of ATM OAM Management cells. This feature allows the routing protocols to take appropriate actions and reroute traffic as a result of a failure in the ATM network.

After the feature is enabled, the F5 OAM alarm indication system (AIS) cells are monitored on the permanent virtual circuit (PVC). If the number of consecutive OAM AIS cells received is greater than a configurable number, the subinterface is brought down. The subinterface is brought up when there is no OAM AIS cell received in a configurable interval.

If the PVC has the end-to-end OAM loopback enabled, the subinterface is brought down after a configurable number of retries. After the OAM loopback succeeds or the far-end loopback request is received, the subinterface is brought up.

**Note**

ATM OAM Management features are only supported on the ATM Port Adapter (PA-A1) and Enhanced ATM Port Adapter (PA-A3), and only for point-to-point subinterfaces (with a single PVC).

ATM OAM features developed in Cisco IOS Release 11.3 T that are in Cisco IOS Release 12.0 are not backward-compatible with the Cisco IOS Release 11.1 CC Limited ATM OAM Management feature. Customers must change their ATM OAM configurations when they upgrade from Cisco IOS Release 11.1 CC to Cisco IOS Release 12.0.

IP to ATM CoS

The IP to ATM Class of Service (CoS) feature implements a solution for coarse-grained mapping of quality of service (QoS) characteristics between IP and ATM, using Cisco PA-A3 ATM port adapters on Cisco 7500 series routers. (This category of coarse-grained QoS is often referred to as class of service.) The resulting feature makes it possible to support differential services in network service provider environments.

IP to ATM CoS is designed to provide a true working solution to class-based services, without the reinvestment of new ATM network infrastructures. Now networks can offer different service classes (sometimes termed “differential service classes”) across the entire WAN (not just the routed portion). Mission-critical applications can be given exceptional service during periods of high network usage and congestion. In addition, noncritical traffic can be restricted in its network usage, which ensures greater quality of service for more important traffic and user types.

With this release of IP to ATM CoS (phase 1), network managers can use existing features (such as Committed Access Rate [CAR] or policy-based routing) to classify and mark different IP traffic by modifying the IP precedence field in the IPv4 packet header. Subsequently, weighted random early detection (WRED) can be configured for each virtual circuit (VC), so that the IP traffic is subject to different drop probabilities (and therefore priorities) as IP traffic coming into a router competes for bandwidth on a particular VC.

PA-A3 ATM port adapters provide the ability to shape traffic on each VC according to the ATM service category and traffic parameters employed. Using the IP to ATM CoS feature, congestion is managed entirely at the IP layer by WRED running on the routers at the edge of the ATM network.

This release of IP to ATM CoS supports a single ATM VC between source and destination ATM end-devices. Multiple IP classes of service can be carried over each VC. A future release of IP to ATM CoS will allow users to build a “VC bundle” that contains multiple VCs between source and destination ATM end-devices. Each VC in the bundle can have different ATM QoS characteristics.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism that connects multiple Protocol Independent Multicast sparse mode (PIM-SM) domains. Each PIM-SM domain uses its own independent Route Processors (RPs) and does not have to depend on RPs in other domains.

Some advantages of this protocol:

- PIM-SM domains can rely on their own RPs only.
- Domains with only receivers get data without globally advertising group membership.
- Global source state is not required.

Documentation on this feature will be available at a later release.

PA-MC-E3 Multi-Channel E3 Port Adapter Enhancement

The PA-MC-E3 Multi-Channel E3 port adapter was announced in Cisco IOS Release 11.1(18)CC. With Cisco IOS Release 11.1(22)CC, in addition to channelized, fractional, and unframed configurations, you can now configure PRI ISDN configurations.

For PRI ISDN configurations, each time slot you assign to a Primary Rate Interface (PRI) group for a configured E1 line uses one of the 128 available logical channels. This includes each time slot within a range of time slots.

For more information on the PA-MC-E3 port adapter, see the *PA-MC-E3 Multi-Channel E3 Port Adapter Installation and Configuration* publication that accompanies the hardware.

New Features in Cisco IOS Release 11.1(21)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(21)CC supports the following new features:

PA-POS-OC3-SML, PA-POS-OC3SMI, and PA-POS-OC3MM Port Adapters

The Packet-over-SONET OC-3 port adapters (PA-POS-OC3-SML, PA-POS-OC3SMI, and PA-POS-OC3MM) are available on Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7500 series routers, and Cisco 7200 series routers. The POS OC-3 port adapter provides a single 155.520-Mbps packet OC-3 network interface.



Note

Although the PA-POS-OC3-SML, PA-POS-OC3SMI, and PA-POS-OC3MM port adapters were announced in Cisco IOS Release 11.1(20)CC, they are only supported in Cisco IOS Release 11.1(21)CC.

For more information on the PA-POS-OC3 port adapters, see the *PA-POS-OC3 Packet OC-3 Port Adapter Installation and Configuration* publication that accompanies the hardware.

New pos ais-shut Command

The **pos ais-shut** interface configuration command controls whether an alarm indication signal-line (AIS-L) is sent when a Packet-over-SONET (POS) interface is shut down. The default behavior is that AIS-L is not asserted. To send AIS-L when a POS line card is shut down, configure the interface with the **pos ais-shut** command. It is possible for an interface to shut down silently (no alarm) if **pos ais-shut** is not configured. Prior to Cisco IOS Release 11.1(21)CC, when a POS interface shut down, the framer was reset. In Cisco IOS Release 11.1(21)CC and later releases of 11.1 CC, the framer is no longer reset when a POS interface is shut down.

For more information on the **pos ais-shut** interface configuration command, see the publication that accompanies the hardware.

PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML Port Adapter Enhancements

The PA-A3 port adapters were introduced in Cisco IOS Release 11.1(19)CC. With Cisco IOS Release 11.1(21)CC, they now support the following:

- Basic Cisco LAN Emulation (LANE) support based on ATM Forum LANE Specification 1.0—This basic LANE support includes IP and IPX protocols only. This LANE support does not include Cisco IOS Release 11.2 or 11.3 Cisco ATM or LANE features such as UNI 3.1, Simple Server Replication Protocol (SSRP), Hot Standby Router Protocol (HSRP), and so forth. Extended AppleTalk is not supported over LANE in this release.
- Dual port adapter configurations in the VIP2-50 for the Cisco 7500 series— Dual port adapter configurations are already supported on both the VIP2-50 and VIP2-40 with the PA-A3-T3 and PA-A3-E3.



Note Dual port adapter configurations with the PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML are not supported on the VIP2-40.

The PA-A3 port adapters are designed to provide maximum switching performance when a single port adapter is installed in a VIP2-50. A single PA-A3 in a VIP2-50 provides up to 85,000 pps of switching capacity in each direction using 64-byte packets.

For applications that require maximum port density or lower system cost, the VIP2-50 now supports any combination of port adapters. Although a single PA-A3 port adapter can use the entire switching capacity of the VIP2-50, dual port adapters in the same VIP2-50 share the 95,000 pps of switching capacity, depending on the port adapters.

Also, the VIP2-50 provides roughly 400 Mbps of aggregate bandwidth. In some dual port adapter configurations with the PA-A3 port adapter, the combination of port adapters exceeds this aggregate bandwidth capacity. Consequently, the VIP2-50 performance is limited by the aggregate switching capacity (95 kbps) at small packet sizes, and by the aggregate bandwidth (400 Mbps) at large packet sizes.

PA-A3-T3 and PA-A3-E3 Port Adapter Enhancements

The PA-A3-T3 and PA-A3-E3 port adapters were introduced in Cisco IOS Release 11.1(18)CC. Basic Cisco LAN Emulation (LANE) support is based on ATM Forum LANE Specification 1.0. This basic LANE support includes IP and IPX protocols only. This LANE support does not include Cisco IOS Release 11.2 or 11.3 Cisco ATM or LANE features such as UNI 3.1, SSRP, HSRP, and so forth. Extended AppleTalk is not supported over LANE in this release.

New Features In Cisco IOS Release 11.1(20)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(20)CC supports the following new features:

PA-MC-T3 Port Adapter

The PA-MC-T3 Multi-Channel T3 port adapter is available on the second-generation Versatile Interface Processor (VIP2) in Cisco 7500 series routers and in Cisco 7000 series routers with the RSP7000 and RSP7000CI installed.

Frame Relay Support for POS Interfaces

The Packet OC-3 Interface Processor (on Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000) and the Packet-over-SONET OC-3 port adapters (on Cisco 7000 series routers with the RSP7000, Cisco 7500 series routers, and Cisco 7200 series routers) support Frame Relay encapsulation.

For more information on the Packet-over-SONET OC-3 port adapters, see the *PA-POS-OC3 Packet OC-3 Port Adapter Installation and Configuration* publication that accompanies the hardware.

For more information on the Packet OC-3 Interface Processor, see the *Packet OC-3 Interface Processor (POSIP) Installation and Configuration* publication that accompanies the hardware.

Multichannel T1/E1 Port Adapter Support

The Multichannel E1 and T1 Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) port adapters (PA-MC-8E1/120, PA-MC-4T1, PA-MC-8T1, and PA-MC-8DSX1) are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with RSP7000 and RSP7000CI.

For more information on these port adapters, see the following publications that accompany the hardware:

- *Multichannel DS1/PRI Port Adapter Installation and Configuration*
- *Multichannel E1/PRI Port Adapter Installation and Configuration*

MAC Address Accounting

MAC Address Accounting provides accounting information for IP traffic based on the source and destination Media Access Control (MAC) address on LAN interfaces. This feature calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent. For example, with this feature you can determine how much traffic is destined for various peers at the network access points. This feature is currently supported on Ethernet, Fast Ethernet, and FDDI interfaces and supports Cisco Express Forwarding (CEF), distributed CEF (dCEF), flow, and optimum switching.

Precedence Accounting

Precedence Accounting provides accounting information for IP traffic based on the precedence of any interface. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on the IP precedence. This feature is supported on all interfaces and subinterfaces and supports CEF, dCEF, flow, and optimum switching.

QoS Policy Propagation Through BGP Enhancements

The Quality of Service (QoS) policy propagation through Border Gateway Protocol (BGP) feature was introduced in Cisco IOS Release 11.1(17)CC. With Cisco IOS Release 11.1(20)CC, the QoS policy propagation through BGP feature has the following enhancements:

- QoS group ID—You can set an internal QoS group ID that can be used later to perform rate-limiting or weighted fair queuing based on the QoS group ID. In the previous release, you could only set up to eight IP precedence levels to classify packets. By setting the QoS group ID in addition to the IP precedence, you can now have more than eight classes on which to perform rate-limiting or weighted fair queuing.
- Source and destination address lookup—You can specify whether the IP precedence level or the QoS group ID used is obtained from the source (input) address or destination (output) address entry in the route table. In the previous release, you could only use the destination address. You can now specify the input or output address.

Fast EtherChannel Enhancements

The following enhancements have been made to the Fast EtherChannel feature:

- Support for host standby using Hot Standby Router Protocol (HSRP)—Available in Cisco IOS Release 11.1(19)CA and Cisco IOS Release 11.1(20)CC
- Support for Cisco Express Forwarding (CEF) and distributed CEF (dCEF)—Available in Cisco IOS Release 11.1(20)CC

Committed Access Rate Enhancements

The Committed Access Rate (CAR) feature was introduced in Cisco IOS Release 11.1(17)CC. With Cisco IOS Release 11.1(20)CC, in addition to classifying packets by setting the IP precedence, you can now also classify packets by setting the QoS group. A QoS group is a QoS class identifier internal to the router.

Distributed Weighted Fair Queuing Enhancements

The distributed weighted fair queuing (DWFQ) feature was introduced in Cisco IOS Release 11.1(17)CC. With Cisco IOS Release 11.1(20)CC, in addition to queuing packets based on the flow, you can now also queue packets based on class. In class-based WFQ, packets are assigned to different queues based on their QoS group or the IP precedence in the type of service (ToS) field. You can customize your QoS policy using QoS groups. A QoS group is an internal classification of packets used by the router to determine how packets are treated by certain QoS features, such as WFQ and CAR. Use a CAR policy or QoS policy propagation through BGP to assign packets to QoS groups. If you want to classify packets based only on the two low-order IP precedence bits, use ToS-based WFQ.

Multicast BGP

Multicast BGP (MBGP) adds capabilities to Border Gateway Protocol (BGP) to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, MBGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by Protocol Independent Multicast (PIM) to build data distribution trees.

It is possible to configure BGP peers that exchange both unicast and multicast network layer reachability information (NLRI).

MBGP is useful when you want a link dedicated to multicast traffic, perhaps to limit which resources are used for which traffic. Perhaps you want all multicast traffic exchanged at one network access point. With MBGP, you can have a unicast routing topology different from a multicast routing topology. Thus, you have more control over your network and resources.

Before MBGP, the only way to do interdomain multicast routing was to use the BGP infrastructure that was in place for unicast routing. If those routers were not multicast capable, or you had differing policies where you wanted multicast traffic to flow, you could not support it.

Multicast Distributed Switching

Prior to multicast distributed switching (MDS), IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms. With Cisco IOS Release 11.2 GS and Cisco IOS Release 11.1 CC, IP multicast traffic can be distributed switched on RSP-based platforms with VIPs.

Furthermore, MDS is the only multicast switching method on the Cisco 12000 Gigabit Switch Router (GSR), starting with Cisco IOS Release 11.2(11)GS.

Switching multicast traffic at the RP has the following disadvantages:

- The load on the RP is increased. This affects important route updates and calculations (for BGP, among others) and can stall the router if the multicast load is significant.
- The net multicast performance is limited to what a single RP can switch.

MDS solves these problems by performing distributed switching of multicast packets received at the line cards (VIPs in the case of an RSP, and line cards in the case of a GSR). The line card is the interface card that houses the VIPs (in the case of an RSP) and the GSR line card (in the case of a GSR). MDS is accomplished using a forwarding data structure called a Multicast Forwarding Information Base (MFIB), which is a subset of the routing table. A copy of MFIB runs on each line card and is always kept up-to-date with the RP MFIB table.

In the case of RSP, packets received on non-VIP interface processors are switched by the RP.

MDS can work in conjunction with Cisco Express Forwarding (CEF), unicast distributed fast switching (DFS), or flow switching.

New Features in Cisco IOS Release 11.1(19)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(19)CC supports the following new features:

PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML Port Adapters

The PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML enhanced ATM port adapters are a new generation of single-width, single-port ATM port adapters available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the RSP7000 and RSP7000CI. The PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML support the following standards-based interfaces:

- OC-3c/STM1 multimode
- OC-3c/STM-1 single-mode intermediate reach
- OC-3c/STM-1 single-mode long reach

The PA-A3 port adapters support all Cisco IOS features and ATM-specific features available in Cisco IOS Release 11.1(18)CC except for the available bit rate (ABR) permanent virtual circuit (PVC) and LAN Emulation (LANE) features. ABR and LANE will be supported in a future maintenance release of Cisco IOS Release 11.1 CC.

The VIP2-40 and VIP2-50 support only one PA-A3-OC3. Support for a second port adapter on a VIP2-50 will be added in a future maintenance release of Cisco IOS Release 11.1 CC.

For more information on the PA-A3 port adapters, see the *PA-A3 Enhanced ATM Port Adapter Installation and Configuration* publication that accompanies the hardware.

Cisco 7202 Router

The Cisco 7202 router is the newest member of the Cisco 7200 series routers, which consist of the two-slot Cisco 7202, four-slot Cisco 7204, and the six-slot Cisco 7206. The Cisco 7202 supports multiprotocol, multimedia routing, and bridging with a wide variety of protocols and any combination of Ethernet, Fast Ethernet, Token Ring, FDDI, ATM, ISDN, and serial media.

Network interfaces reside on port adapters that provide the connection among the three Peripheral Component Interconnect (PCI) router buses and external networks. The Cisco 7202 has two slots (slot 1 and slot 2) for the port adapters, one slot for an input/output (I/O) controller, and one slot for a network processing engine. You can place the port adapters in either of the two available slots.



Note

You can install an I/O controller with or without a Fast Ethernet port in all Cisco 7200 series routers; however, when you install an I/O controller with a Fast Ethernet port in a Cisco 7202, the system software automatically disables the port.

There are bays for up to two AC-input or DC-input power supplies. The Cisco 7202 can operate with only one power supply. Although a second power supply is not required, it allows load sharing and increased system availability.

The Cisco 7202 provides the following features:

- Online insertion and removal (OIR)—You can add, replace, or remove port adapters without interrupting the system or entering any console commands.
- Dual hot-swappable, load-sharing power supplies—If one power supply or power source fails, the other power supply maintains system power without interruption by providing system power redundancy. Also, when one power supply is powered off and removed from the router, the second power supply immediately takes over the router's power requirements without interrupting normal operation of the router.
- Environmental monitoring and reporting functions—You can maintain normal system operation by resolving adverse environmental conditions before any loss of operation.
- Downloadable software—For fast, reliable upgrades you can load new images into Flash memory remotely, without having to physically access the Cisco 7202 router.

For additional information, see the *Cisco 7202 Installation and Configuration Guide*.

New Features in Cisco IOS Release 11.1(18)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(18)CC supports the following new features:

Distributed Cisco Express Forwarding NetFlow

The distributed Cisco Express Forwarding (dCEF) NetFlow feature allows the VIP2 to perform NetFlow switching of packets and perform NetFlow data export similar to Cisco Express Forwarding (CEF) flow switching on the RSP. Each VIP2 maintains its own independent flow cache and can generate its own export packets containing statistics on expired flows. Use the **show ip cache flow** command to display per-protocol statistic summaries for packets switched by the RSP and VIP. The **show ip cache flow** command shows only flow details for RSP-switched flows.

If you want to gather dCEF NetFlow data export with the Cisco NetFlow FlowCollector product, you must have FlowCollector Release 2.0.

NetFlow Enhancements

To allow the NetFlow data export collection applications to distinguish between export record sequence numbers sent by different VIP2s, the export format has been changed. Previously there was a 32-bit reserved field in the header of Version 5 export datagrams that was always zero. This field has been split into an 8-bit export engine type, an 8-bit engine ID, and a 16-bit reserved field. You can use the datagrams and the ID field to distinguish between different VIP2s. Flows exported by an RSP card have a zero type and ID that matches the previous 0 value exported by earlier Cisco IOS software. The VIP2s have an export engine type of 1 and an engine ID that corresponds to the slot number of the VIP2.

Table 6 lists the Version 5 header formats.

Table 6 **Version 5 Header Formats**

Bytes	Content	Description
0–1	version	NetFlow export format version number
2–3	count	Number of flows exported in this packet (1–30)

Table 6 Version 5 Header Formats (continued)

Bytes	Content	Description
4–7	SysUptime	Current time in milliseconds since router booted
8–11	unix_secs	Current seconds since 0000 UTC 1970
12–15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16–19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow switching engine
21	engine_id	Slot number of the flow switching engine
22–23	reserved	Unused (zero) bytes

PA-A3-T3 and PA-A3-E3 Port Adapters

The PA-A3-T3 and PA-A3-E3 enhanced ATM port adapters are a new generation of single-width, single-port ATM port adapters available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the RSP7000 and RSP7000CI. The PA-A3-T3 provides one high-speed DS3 interface, and the PA-A3-E3 provides one medium-speed E3 interface.

The PA-A3-T3 and PA-A3-E3 port adapters support all Cisco IOS features and ATM-specific features available in Cisco IOS Release 11.1(18)CC except for the available bit rate (ABR), permanent virtual circuit (PVC), and LAN emulation (LANE) features. ABR and LANE will be supported in a future maintenance release of Cisco IOS Release 11.1 CC.

PA-MC-E3 Multi-Channel E3 Port Adapter

The PA-MC-E3 Multi-Channel E3 synchronous serial port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the RSP7000 and RSP7000CI. The PA-MC-E3 has one channelized E3 high-speed serial interface that provides access to services at E1 (2.048 Mbps) data rates, transferring data bidirectionally. This port adapter divides the E3 signal stream into 16 E1 lines that can be further divided to the 64-kbps level, up to a total of 128 channels. The PA-MC-E3 complies with ITU-T/ITU G.703 physical layer standards and ITU-T/ITU G.751 for E3, G.742 for E2, and G.704 and G.706 for E1 fault and alarm detection and response actions.

The E1 lines can be configured as channelized, fractional, and unframed.

New Features in Cisco IOS Release 11.1(17)CC

In addition to the features in Cisco IOS Release 11.1 CA, Cisco IOS Release 11.1(17)CC supports the following new features:

Cisco Express Forwarding

Cisco Express Forwarding (CEF) is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, networks characterized by intensive Web-based applications, or interactive sessions. Although you can use CEF in any part of a network, it is designed for high-performance, highly resilient Layer 3 IP backbone switching.

Committed Access Rate

Committed Access Rate (CAR) performs the following functions:

- Limits the input or output transmission rate on an interface or subinterface based on a flexible set of criteria
- Classifies packets by setting the IP precedence

CAR can be used to rate-limit traffic based on packet characteristics such as access list, incoming interface, or IP precedence. CAR provides configurable actions such as transmit, drop, or set precedence when traffic conforms to or exceeds the rate limit.

Distributed Weighted Random Early Detection

Random early detection (RED) is a congestion-avoidance mechanism that takes advantage of the TCP congestion-control mechanism. By randomly dropping packets before periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it decreases its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED) drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher-priority traffic is delivered with a higher probability than lower-priority traffic.

WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than the edge. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how it treats different types of traffic.

Distributed WRED (DWRED) uses the VIP rather than the RSP to perform the queuing; therefore, it requires a Cisco 7500 series router or Cisco 7000 series router with the RSP7000.

Distributed Weighted Fair Queuing

Weighted fair queuing (WFQ) controls the ratio of transmission bandwidth allocation among different traffic flows during periods of congestion. Distributed WFQ (DWFQ) uses the VIP rather than the RSP to perform the queuing; therefore, it requires a Cisco 7500 series router or Cisco 7000 series router with the RSP7000.

Automatic Protection Switching of Packet-over-SONET Circuits

Automatic Protection Switching (APS) is supported on Cisco 7500 series routers. This feature allows switchover of Packet-over-SONET (POS) circuits and is often required when connecting SONET equipment to telco equipment. APS refers to the mechanism of bringing a “protect” POS interface into the SONET network as the “working” POS interface on a circuit from the intervening SONET equipment.

The protection mechanism used for this feature is “1+1, Bidirectional, nonrevertive” as described in the Bellcore publication *TR-TSY-000253, SONET Transport Systems: Common Generic Criteria, Section 5.3*. In the 1+1 architecture, there is one working interface (circuit) and one protect interface, and the same payload from the transmitting end is sent to both receiving ends. The receiving end decides which interface to use. The line overhead bytes (K1 and K2) in the SONET frame indicate both status and action.

The protect interface is configured with the IP address of the router that has the working interface. The APS Protect Group Protocol, which runs on top of User Datagram Protocol (UDP), provides communication between the process controlling the working interface and the process controlling the protect interface. With this protocol, POS interfaces can be switched because of a router failure, degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair. In unidirectional mode, the transmit and receive channels are switched independently. For example, if the receive channel on the working interface has a loss of channel signal, both the receive and transmit channels are switched.

In addition to the new Cisco IOS commands added for the APS feature, the POS interface configuration commands, **pos threshold** and **pos report**, have been added to support user configuration of the bit error rate (BER) thresholds and reporting of SONET alarms.

QoS Policy Propagation Through BGP

With Quality of Service (QoS) policy propagation through Border Gateway Protocol (BGP), you can classify packets based on access lists, BGP community lists, and BGP autonomous system paths. The supported classification policies include IP precedence setting and the ability to tag the packet with a QoS class identifier internal to the router (available in a future maintenance release of the software). After a packet has been classified, you can use other QoS features such as CAR and WRED to specify and enforce business policies to fit your business model.

Expanded IP Access Lists

This feature expands the extended IP access list range as follows:

- 1–99: IP standard access list
- 100–199: IP extended access list
- 1300–1999: IP standard access list (expanded range)
- 2000–2699: IP extended access list (expanded range)

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 7](#).

Table 7 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1234-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

This section contains important information about the Cisco IOS Release 11.1 CC software. The following information describes the changes by release number for Cisco IOS Release 11.1 CC:

Image Obsolescence, Cisco IOS Release 11.1(36)CC2

All Cisco 7200 series and Cisco 7500 series images in Cisco IOS Releases 11.1(36)CC1 have been obsoleted from manufacturing due to the following caveats:

- CSCdt11503—IOS crashes when large OID (>256 fields) is received
- CSCdt51376—New appn subsystem object files for 11.1(36)CC1
- CSCdt79947—Core router crashes with memory corruption
- CSCdt93866—Unchecked limits in NTP

These images are now available in Cisco IOS Release 11.1(36)CC2.



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.

Image Obsolescence, Cisco IOS Release 11.1(36)CC1

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

- CSCds04747

These images are now available in Cisco IOS Release 11.1(36)CC1.



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 CC

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 CC is scheduled to reach End of Sales with maintenance release 11.1(35)CC, and will no longer be orderable as of September 15, 2000. Note that Cisco IOS Release 11.1 CC images will remain posted on CCO after EOS, though they will no longer be orderable with new systems. Cisco IOS Release 11.1 CC will reach End of Engineering with maintenance release 11.1(36)CC5.

If all required features and hardware are supported, evaluate Cisco IOS Software Release 12.0, which is now the preferred GD-certified release for the Cisco 7200 and Cisco 7500 platforms. Cisco IOS Release 12.0 contains most Cisco IOS Release 11.1 CC features and hardware support.

Service providers requiring additional features and hardware not available in release 12.0 should evaluate Cisco IOS release 12.0S. Cisco IOS Release 12.0 S is based on Cisco IOS Release 12.0, with additional service provider-focused features and hardware support. Note that only Service Provider images are available in 12.0S, and these images are only available for Cisco 7200 series, Cisco 7500 series, and Cisco 12000 series platforms.

If additional hardware and software feature support is required, evaluate Cisco IOS Software Release 11.1 CC features as well as all 12.0 and 12.0T features, and offers a broad variety of feature sets, including Enterprise multiprotocol, Cisco IOS Firewall feature set, and IPsec encryption.

For more information about the EOS and EOE of Cisco IOS Software Release 11.1 CC, refer to the Product Bulletin located on CCO at:

http://www.cisco.com/warp/customer/cc/pd/rt/platform/prodlit/1122_pp.htm

Image Obsolescence, Cisco IOS Release 11.1(33)CC

Cisco IOS Release 11.1(33)CC was obsoleted to Cisco IOS Release 11.1(33)CC1 on all software images to incorporate corrections to the following caveat:

CSCdr36952—<http://router-ipaddr/%%> crashes router hard

A Cisco router may reload or pause indefinitely when the IOS HTTP service is enabled and a browser connects to <http://<router-ip>/%%>. This may be exploited to produce a denial of service (DoS) attack.

Workaround 1: Disable the ip http server with the **no ip http server** command.

Workaround 2: Block port 80 connections to the router via access lists or other firewall methods.

For further information, refer to the Internet Security Advisory located at the following URL:

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

Cisco IOS Release 11.1(32)CC MIB Modification

The CISCO CAR MIB has been modified in Cisco IOS Release 11.1(32)CC to include 64-bit counters because of the following caveat:

CSCdp91476—Request for 64 bit CAR MIB counters

Cisco IOS Release 11.1(30)CC Release Cycle Change

Cisco IOS Release 11.1(30)CC is the first 11.1 CC release to be released two weeks after the corresponding 11.1 CA release.

Image Deferral, Cisco IOS Release 11.1(29)CC

Cisco IOS Release 11.1(29)CC was deferred to Cisco IOS Release 11.1(29)CC1 on all software images to incorporate corrections to the following caveats:

- CSCdp13010—CBus complex restart occurs minutes after boot
- CSCdp13469—PODIA T3 PA Not doing distributed switching after OIR on other PA/VIP

For additional information on Cisco IOS Release 11.1 deferrals, including the Cisco IOS Release 11.1(29)CC deferral, see the *What's Hot for Cisco IOS Software Release 11.1* documentation at CCO. To reach the *What's Hot for Cisco IOS Software Release 11.1* document, log in to CCO and follow this path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS 11.1: What's Hot for Cisco IOS Software Release 11.1

Image Deferral, Cisco IOS Release 11.1(28)CC

Cisco IOS Release 11.1(28)CC was deferred to Cisco IOS Release 11.1(29)CC on all RSP images (rsp-v*) because of the following caveat:

CSCdm88958—RSP HSA SYNC Configuration fails with Slave configuration write error (0)

For more information refer to the field notice located at the following URL:

http://www.cisco.com/warp/customer/770/fn7431_09161999.shtml

For more information on CSCdm88958, refer to the Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, log in and follow this path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II

Release Cycle Change

Cisco IOS Release 11.1(27)CC was released separately but at the same time as Cisco IOS Release 11.1(28)CC due to a change in the release cycle of Cisco IOS Release 11.1 CC from thirteen to seven weeks.

Image Deferral, Cisco IOS Release 11.1(26)CC

Cisco IOS Release 11.1(26)CC was deferred to Cisco IOS Release 11.1(26)CC1 on all software images to incorporate corrections to the following caveat:

- CSCdm38024—FIP keeps resetting when HSRP, CDP, and so on are not configured

For additional information, log in to CCO and refer to *What's Hot for Cisco IOS Software Release 11.1* located at the following path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS 11.1: What's Hot for Cisco IOS Software Release 11.1

A field notice providing information on CSCdm38024 is located at the following URL:

http://www.cisco.com/warp/public/770/fn5168_06091999.shtml

For more information on this caveat, refer to the Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, follow this path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II

Early Deployment Release, Cisco IOS Release 11.1(21)CC2

Cisco IOS Release 11.1(21)CC2 is an early deployment release of software support for the Cisco 7000 family. Cisco IOS Release 11.1(21)CC2 is the same as Cisco IOS Release 11.1(21)CC, except the following defects have been resolved in Cisco IOS Release 11.1(21)CC2:

- CSCdj35146—VIP crash info shows all zeros in registers content
- CSCdj50021—Route-map and filter-list cache busted, results in route leg
- CSCdj82421—Mroute-cache corruption in AIP

- CSCdj87399—RSP2 crash at crashdump after enable debug arp
- CSCdj94991—POSIP crash at vip_pak_to_host_inline
- CSCdk02186—Crash in rsp_ipfastswitch after interface flap, c.encaps=NUL
- CSCdk11206—Cisco 7500 configured with HSRP crashed at bootup
- CSCdk11808—Dialer idle-timeout does not work on a Cisco 7200 series router with 4T+
- CSCdk13965—CT3IP: Spurious accesses in ct3_periodic()
- CSCdk18176—Bus error when bridging on ATM interface
- CSCdk27922—ATM-lite Rx errors (ignored) after peer reset
- CSCdk29300—Process DVMRP prunes to unicast addresses on point-to-point interfaces
- CSCdk30189—RSP2 crash at atm_getvc_deleted when enable/dis DWRED per Vt
- CSCdk32520—Ip dvmrp metric <n> should only inject directly connected rs
- CSCdk34967—POSPA: interface should be admin down when inserted with no cable
- CSCdk35200—Icmp redirect not working with CEF enabled
- CSCdk35564—Extended access-list failure, DFS switching out a legacy IP
- CSCdk35821—Spurious accesses in show diag code
- CSCdk39936—Fast Ethernet needs to report correct line status
- CSCdk40099—CT3PA:VIP2 crashed at ct3sw_fastsend_inline() by changing Tg
- CSCdk41173—New application subsystem object files for Release 11.1(21)CC
- CSCdk41546—PA-MC-T1 does not work in AMI and 56K speed, same with PA3
- CSCdk43485—Complete cleanup of path information after detecting bad ate
- CSCdk43862—DFS/multiple outbound ACL on subinterfaces could use incorL
- CSCdk43920—Command history release at login prompt
- CSCdk44597—ATM Lite: OAM loopback not working on PVC
- CSCdk48525—POET (packet over 53/Ts3) drops at low data rates when combined with a subrate POET

For additional information, log in to CCO and refer to What's Hot for Cisco IOS Software Release 11.1 located at the following path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS 11.1: What's Hot for Cisco IOS Software Release 11.1

For more information on these caveats, refer to the Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, follow this path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II

A field notice providing information on early deployment release 11.1(21)CC2 is located at the following URL:

<http://www.cisco.com/warp/public/770/fa111-21cc1.shtml>



Note

Field Notice: Cisco IOS Release 11.1(21)CC2 replaces Field Notice: Cisco IOS Release 11.1(21)CC1.

Early Deployment Release, Cisco IOS Release 11.1(19)CC1

Cisco IOS Release 11.1(19)CC1 is an early deployment release of software support for the Cisco 7000 family. Cisco IOS Release 11.1(19)CC1 is the same as Cisco IOS Release 11.1(19)CC except the following defects have been resolved in Cisco IOS Release 11.1(19)CC1:

- CSCdj77694—Router forwards packets out of sequence with WFQ.
- CSCdk10629—EIGRP: HELLO packets could not go out on HSSI/4T with fair queue enabled.
- CSCdj95348—In some situations weighted fair queuing (WFQ) might drop Open Shortest Path First (OSPF) and EIGRP HELLO messages, causing the protocol to go down.

Workaround: Disable WFQ on the interface.

- CSCdk10140—The OC-3 PA-A3 interface might stay down in a back-to-back connection if both ends perform a “micro reload” or a **shut/no shut** command at about the same time. This is the first release that supports OC-3 PA-A3.
- CSCdk10114—Tearing down a VC supported by a PA-A3 when the line is down might cause Cisco 7200 series routers to reload.

Workaround: Do not change the VC configuration when the line is down.

- CSCdk10016—The OC-3 PA-A3 throughput might be reduced if TCP decreases its window size because of a packet drop that is caused by the SAR RX cell throttle.
- CSCdk10961—The router reloads when the VIP is really low on memory and unable to malloc error buffers for stats download to the RP.
- CSCdk10303—Added new Advanced Peer-to-Peer Networking (APPN) subsystem objects files for the Release 11.1(19)CC build.

For additional information, log in to CCO and refer to *What's Hot for Cisco IOS Software Release 11.1* located at the following path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS 11.1: What's Hot for Cisco IOS Software Release 11.1

For more information on these caveats, refer to the Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, follow this path:

Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II

A field notice providing information on CSCdk10629 is located at the following URL:

<http://www.cisco.com/warp/customer/770/fa-rsp-k10629.shtml>

Minimum Recommended Releases

These release notes list 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 sometimes the change is to correct caveats.

The hardware documentation that ships with the port adapter or interface processor lists the minimum release of Cisco IOS software required to support the port adapter, which might not be the Cisco IOS release 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.

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 CCare also in Cisco IOS Release 11.1(36)CC5.

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 CC1.



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 8 Caveats Reference for Cisco IOS Release 11.1 CC

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdi74403	X	
CSCdi88756	X	
CSCdj03047	X	
CSCdj18292	X	
CSCdj18685	X	
CSCdj20995	X	
CSCdj23230	X	
CSCdj26511	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdj31863	X	
CSCdj32533	X	
CSCdj33812	X	
CSCdj34203	X	
CSCdj35146	X	
CSCdj45202	X	
CSCdj50021	X	
CSCdj52309	X	
CSCdj58132	X	
CSCdj59639	X	
CSCdj60905	X	
CSCdj68602	X	
CSCdj69073	X	
CSCdj69424	X	
CSCdj69939	X	
CSCdj70296	X	
CSCdj71438	X	
CSCdj71597	X	
CSCdj75305	X	
CSCdj75596	X	
CSCdj75983	X	
CSCdj76100	X	
CSCdj76595	X	
CSCdj77694	X	
CSCdj77846	X	
CSCdj79452	X	
CSCdj79497	X	
CSCdj79565	X	
CSCdj79992	X	
CSCdj82421	X	
CSCdj83578	X	
CSCdj83777	X	
CSCdj87399	X	
CSCdj88375	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdj88927	X	
CSCdj91037	X	
CSCdj91100	X	
CSCdj94991	X	
CSCdj95348	X	
CSCdk02186	X	
CSCdk02527	X	
CSCdk04126	X	
CSCdk06529	X	
CSCdk06571	X	
CSCdk07174	X	
CSCdk09038	X	
CSCdk10016	X	
CSCdk10114	X	
CSCdk10140	X	
CSCdk10303	X	
CSCdk10629	X	
CSCdk10665	X	
CSCdk10713	X	
CSCdk10762	X	
CSCdk10948	X	
CSCdk10961	X	
CSCdk11206	X	
CSCdk11808	X	
CSCdk13965	X	
CSCdk18176	X	
CSCdk19805	X	
CSCdk22030	X	
CSCdk22991	X	
CSCdk23648	X	
CSCdk25121	X	
CSCdk25825	X	
CSCdk27330		X
CSCdk27922	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdk28971	X	
CSCdk29300	X	
CSCdk30189	X	
CSCdk30727	X	
CSCdk30791	X	
CSCdk32520	X	
CSCdk34128	X	
CSCdk34319	X	
CSCdk34549	X	
CSCdk34967	X	
CSCdk35200	X	
CSCdk35821	X	
CSCdk36161	X	
CSCdk37522	X	
CSCdk39920	X	
CSCdk39936	X	
CSCdk40049	X	
CSCdk40099	X	
CSCdk41173	X	
CSCdk41546	X	
CSCdk41648	X	
CSCdk43485	X	
CSCdk43862	X	
CSCdk43920	X	
CSCdk44523	X	
CSCdk44597	X	
CSCdk47218	X	
CSCdk47375	X	
CSCdk48525	X	
CSCdk50463	X	
CSCdk51304	X	
CSCdk54265	X	
CSCdk54312	X	
CSCdk57889	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdk58799	X	
CSCdk59118	X	
CSCdk60164	X	
CSCdk61320	X	
CSCdk61689	X	
CSCdk62487	X	
CSCdk63163	X	
CSCdk63661	X	
CSCdk65504	X	
CSCdk67183	X	
CSCdk67709	X	
CSCdk68604	X	
CSCdk69045	X	
CSCdk69452		X
CSCdk71109	X	
CSCdk72452	X	
CSCdk72928	X	
CSCdk74144	X	
CSCdk74680	X	
CSCdk74808	X	
CSCdk75670	X	
CSCdk76192	X	
CSCdk76520	X	
CSCdk77016	X	
CSCdk77704	X	
CSCdk78845	X	
CSCdk79642	X	
CSCdk79774	X	
CSCdk79957	X	
CSCdk79961	X	
CSCdk80974	X	
CSCdk81576	X	
CSCdk81888	X	
CSCdk82659	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdk83363	X	
CSCdk83829	X	
CSCdk88162	X	
CSCdk89734	X	
CSCdk90244	X	
CSCdk92886	X	
CSCdk93443	X	
CSCdm01124	X	
CSCdm01617	X	
CSCdm02157	X	
CSCdm05197	X	
CSCdm05440	X	
CSCdm06448	X	
CSCdm07023	X	
CSCdm10790	X	
CSCdm11933	X	
CSCdm14098	X	
CSCdm18492	X	
CSCdm18977	X	
CSCdm19573	X	
CSCdm20127	X	
CSCdm24099	X	
CSCdm24286	X	
CSCdm25426	X	
CSCdm28550	X	
CSCdm28893	X	
CSCdm29580	X	
CSCdm29755	X	
CSCdm32171	X	
CSCdm35733	X	
CSCdm37878	X	
CSCdm38024	X	
CSCdm40249	X	
CSCdm42165	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdm44772	X	
CSCdm45233	X	
CSCdm46655	X	
CSCdm51483	X	
CSCdm53977	X	
CSCdm55716	X	
CSCdm57609	X	
CSCdm57759	X	
CSCdm58335	X	
CSCdm64005	X	
CSCdm67167	X	
CSCdm67344	X	
CSCdm69594	X	
CSCdm71133	X	
CSCdm71799	X	
CSCdm71880	X	
CSCdm78036	X	
CSCdm84162	X	
CSCdm88958	X	
CSCdp01551	X	
CSCdp02958	X	
CSCdp03602	X	
CSCdp08290	X	
CSCdp09645	X	
CSCdp13010	X	
CSCdp13469	X	
CSCdp14019	X	
CSCdp15196	X	
CSCdp15392	X	
CSCdp24657	X	
CSCdp33774	X	
CSCdp36092	X	
CSCdp43247		X
CSCdp46465	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdp47089	X	
CSCdp49869	X	
CSCdp52532	X	
CSCdp55810	X	
CSCdp60859	X	
CSCdp70710	X	
CSCdp71532	X	
CSCdp74511	X	
CSCdp77490	X	
CSCdp82244	X	
CSCdp83682	X	
CSCdp88255	X	
CSCdp91476	X	
CSCdp97805	X	
CSCdr06665	X	
CSCdr09895	X	
CSCdr11784	X	
CSCdr23540	X	
CSCdr24768	X	
CSCdr30942	X	
CSCdr36952	X	
CSCdr49601	X	
CSCdr51074	X	
CSCdr54230	X	
CSCdr73797	X	
CSCdr81925	X	
CSCdr87607	X	
CSCdr93224	X	
CSCds04747	X	
CSCds09952	X	
CSCdt11503	X	
CSCdt51376	X	
CSCdt79947	X	
CSCdt93866	X	

Table 8 Caveats Reference for Cisco IOS Release 11.1 CC (continued)

DDTS Number	Software Release	
	11.1 CC	
	Caveat Corrected	Caveat
CSCdw65903	X	
CSCdw78210	X	

Resolved Caveats—Cisco IOS Release 11.1(36)CC7

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CC7.

- CSCea02355

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>

Resolved Caveats—Cisco IOS Release 11.1(36)CC5

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CC5. 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-snmp-msgs-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)CC4

This section documents possible unexpected behavior by Cisco IOS Release 11.1(36)CC4 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)CC4.

Resolved Caveats—Cisco IOS Release 11.1(36)CC4

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CC4. 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)CC2

This section documents possible unexpected behavior by Cisco IOS Release 11.1(36)CC2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdk69452

In rare instances, a configuration that uses regular expressions might cause the regular expression-matching routine to enter into an infinite loop that results in a software-forced reload. There are no workaround.

- CSCdp43247

A PA-MC-8E1 may drop packets and have a high latency when the average transmit rate is low. There are no workaround.

- CSCdr23540

A Cisco 7500 series router may reload due to a bus error in `bgp_send_update` after an interface flap. This is a rare condition.

There are no workaround.

- CSCdk27330

If the following command sequence is applied to the controller on a CT3IP, the VIP might reload:

```
t1 external
3 linecode b8zs cablelength 100
no t1 3 timeslots 1-24
no t1 3 clock source line
```



Note All commands entered for this channel after the `no t1 3 timeslots 1-24` command might cause the VIP to reload.

Workaround: To prevent the controller from reloading, issue the commands in the following order:

```
no t1 3 clock source line
t1 external 3 linecode b8zs cablelength 100
no t1 3 timeslots 1-24
```

or

```
no t1 3 clock source line
no t1 3 timeslots 1-24
t1 external 3 linecode b8zs cablelength 100
```



Note Issue the `no t1 3 timeslots 1-24` command after the `no t1 3 clock source line` command.

Resolved Caveats—Release 11.1(36)CC1

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CC2. This section only describes severity 1 and 2 caveats:

- CSCdm46655

A Cisco 7200 series router with PA-F HW rev. 1.13 or 1.14 running Cisco IOS Release 11.1(22)CC may exhibit a condition in which the interface stops transmitting packets on the FDDI interface. The condition can be detected by the lack of output traffic on the interface and output drops increasing on the interface. The output queue from the **show interface** command displays something similar to 40/40.

Workaround: Administratively shut down the FDDI interface with a **shutdown** command followed by a **no shutdown** command.

- 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)CC Through 11.1(36)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(36)CC1. This section only describes severity 1 and 2 caveats:

- CSCdj88375

A router might become unresponsive while copying an image to boot Flash memory using the **copy rcp bootflash** command. There is no workaround.

- CSCdm18492

A Cisco 7000 series router might experience high CPU usage at an interrupt level with flow switching on because of spurious accesses by the flow switching code.

Workaround: Turn off flow switching by using the **no ip route-cache flow** command.

- CSCdp83682

A Route Switch Processor (RSP4) running Cisco IOS Release 11.1(29)CC1 might reload while copying an image to bootflash. There is no workaround.

- CSCdr30942

A Cisco 7200 series router running Cisco IOS Release 11.1 CC with an NPE-200 and a large amount of low-speed serials suffers memory allocation failures, which require a reload of the router to return it to normal operation. After a period of time, the memory allocation failures return. There is no workaround.

- CSCdm32171

When installing a High-Speed Serial Interface (HSSI) and a Packet-over-SONET (POS) port adapter in the same VIP, the HSSI interface may not come up after the POS interface is configured. If the HSSI interface is already up before the POS interface is configured, it might go down and stay down.

Workaround: Do not place HSSI and POS high-speed serial port adapters in the same VIP.

- CSCdp08290
POS output packet counters do not show the correct values.
Workaround: Use the **clear counters pos** command to clear the output packet counters.
- CSCdk51304
A Cisco router might reload or display physical errors after shutting down a controller. When dCEF is enabled on Internet routers, the counters on access lists are not incrementing. There is no known workaround.
- 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>.
- CSCdr93224
A Cisco 7500 series router may experience flapping on the serial interfaces after an online insertion and removal (OIR) of a VIP2-50 with a PA-A3-OC3 port adapter installed. The Fiber Distributed Data Interface (FDDI) may fail to receive any routing updates via OSPF, although it continues to send updates successfully.
Workaround: Reload the router.
- CSCds09952
A VIP2 with a PA-A3 port adapter installed on a Cisco 7513 series router may reload with a bus error exception after an operator initiated reload of the router. The VIP2 becomes operational again approximately five minutes after the reload. There is no workaround.

Resolved Caveats—Release 11.1(1)CC Through 11.1(35)CC

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

- CSCdr73797
A Cisco 7200 series router running Cisco IOS Release 11.1(34)CC might experience Detection of Thrashing condition needs to be reworked in the scheduler (CSCdj68470). Fix needs to be integrated in 11.1CC release.
- CSCdp71532
A Cisco 7500 series router with POS interfaces experiences performance degradation and high CPU utilization when CEF is configured on the POS interface.
Workaround: Remove CEF switching.
- CSCdm25426
There is no route entry in the **show ip cache optimum** command when optimum switching is used on a PA-FE port adapter on a Cisco 7200 series router. This is seen in Cisco IOS Release 11.1(25)CC and not seen in Cisco IOS Release 11.1(25)CA. There is no workaround.
- CSCdr81925
A Cisco 7500 series router with Hot Standby Router protocol (HSRP) configured over the port channel does not detect the standby router. There is no workaround.
- 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)CC Through 11.1(34)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(35)CC. This section only describes severity 1 and 2 caveats:

- CSCdr11784

If you configure Protocol Independent Multicast (PIM) or Hot Standby Router Protocol (HSRP) on an ATM-LANE interface, the CPU of the Route Switch Processor (RSP) might reach 99 percent. This situation only occurs when Open Shortest Path First (OSPF) is enabled on more than 12 interfaces in combination with ATM-LANE. This situation does not occur on an RSP that is running Cisco IOS Release 12.0 S or Release 11.2 GS. There is no workaround.

- CSCdr51074

A Cisco router running Cisco IOS Release 11.1CC may reload with tcp_* functions on the stack when Multicast Source Discovery Protocol (MSDP) over TCP sessions flap. The session flapping is frequently the result of TCP output queue build up (i.e. too many MSDP SA messages, network congestion).

Workaround: Reduce the MSDP Source-Active (SA) traffic by setting up SA filters or upgrading to Cisco IOS Release 12.0S.

- CSCdr54230

A Cisco router may not detect Border Gateway Protocol (BGP) updates with bad AS_PATH attributes. A BGP UPDATE contains network layer reachability information (NLRI) and attributes that describe the path to the destination. Each path attribute is a Type-Length-Value (TLV).

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented itself by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASs) in the segment. The path segment value contains the list of ASs (each AS is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of ASs in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASs (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The defect found was due to the mishandling of the operation described above, during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its BGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

[Part of the text was taken from RFC 1771.]

There is no workaround once the UPDATE with the long AS_PATH enters a network. As the AS_PATH grows, the session resets will be encountered in the AS where the length of the attribute becomes greater than 255.

The solution includes two parts:

- Fix to avoid corruption of the updates.
- Use the **[no] bgp maxas-limit 1-20** configuration command to filter UPDATES based on the total number of ASs in the AS_PATH. This command should be used in router configuration mode. By default there is no limit. If the number of ASs in the AS_PATH exceeds the limit, the UPDATE is stored in the BGP table, but not used in the bestpath selection or propagated. For example, if the limit is set to 20, the router displays:

```
router# sh ip bgp 2.1.1.0 BGP routing table entry for 2.1.1.0/24, version 214
Paths: (1 available, no best path) 10 3 4 3 3 3 5 7 2 8 3 4 4 3 2 6 8 5 6 5 2 1 8
5 2 3 7 4 9 4 6 1 6 9 9 7 5 7 4 9 6 43 22 76 4 9 6 4 7 3 5 2 4 98 0 76 3 4 6 8 9 4
2 1 3 42 8 6 5 6 9 5 5 6 87 5 5 8 5 9 86 3 2 5 2 3 5 4 7 9 6 76 7 8 6 5 8 6 97 7 3
95 3 2 8 7 74 5 8 6 3 3 1 4 9 5 2 3 5 7 4 3 5 2 5 5 7.7.7.7 from 7.7.7.250
(16.1.3.2) Origin IGP, localpref 100, valid, external, maxas-limit <<<<<<
```

While the fix guarantees that the UPDATES will not be corrupted in the local network, the problem may just be propagated to the next AS. It is recommended that you use the **bgp maxas-limit** command at the edge of the network especially in links where routers are peering with suspect BGP implementations.

- CSCdk89734
The Gigabit Ethernet Interface Processor (GEIP) does not support protocols that use the Ethernet 802.3x header TypeLength field as the size for the maximum transmission unit (MTU). This includes SNAP, CLNS, IPX, SDE, IBMNM, and NetBIOS. There is no workaround.
- CSCdp01551
Under certain conditions a Cisco 7200 series router or a VIP with a Multichannel T1 or E1 port adapter will reload when the software on the port adapter pauses indefinitely. There is no workaround.
- CSCdp82244
On a Cisco 7200 series router, the serial drivers may cause a memory leak when a reparented packet is transmitted. There is no workaround.
- CSCdr24768
CEF may not process an interface up event, resulting in a **show interface** command displaying the interface as up while the **show cef interface** command displays the same interface as down. This may result in missing prefixes in the CEF table.
Workaround: Repeat the **no shutdown** command on the interface. It is not necessary to first issue a **shutdown** command on the interface.
- CSCdr49601
A Gigabit Ethernet Interface Processor (GEIP) on a Cisco 7500 series router may experience receive problems causing it to pause indefinitely.
Workaround: Disable dCEF on the GE interface.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(33)CC1

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(34)CC. This section only describes severity 1 and 2 caveats:

- CSCdp47089

An RSP4 may pause indefinitely when a **write memory** command is issued to a configuration file that is greater than 128K and does not have the **service internal** and **service compress-config** commands enabled.

Workaround: Issue the **service internal** and **service compress-config** commands to enable compression.

- CSCdp77490

A Cisco router running Cisco IOS Release 11.1(29)CC1 using Data-Link Switching (DLSw+) border peering over TCP may experience diminished memory resources during periods of network congestion that may result in degraded performance or even a router reload due to memory exhaustion. There is no workaround.

- CSCdp14019

A PA-CT3 port adapter may experience a CPUHOG error during a TFTP download of a Cisco IOS Release 11.1(29) CC image causing the download to fail. There is no workaround.

- CSCdp97805

When a bad transmit packet is generated and sent to the Channelized T3 (CT3) interface, the packet might cause the address of the transmit queue accumulator (txacc) value to increment incorrectly for the CT3 interface. In this situation, the output eventually becomes stuck when the txacc value reaches zero.

Workaround: Configure the CT3 interface with the **tx-queue-limit 5** interface configuration command to restore the txacc value for the affected CT3 interface.

- CSCdk34319

After highly stressing packets through a PA-A3 port adapter on a Cisco 7200 series router, if you remove the card and reinsert it to a different slot with a new configuration on the same interface at the new slot, the router may reload with the following error patterns occurring on the console:

```
%SYS-2-LINKED: Bad enqueue of 60DFD980 in queue 60CCFB30 -Process= "<interrupt
level>", ipl= 1 -Traceback= 602398F0 601C1370 602000C8 60203958 601C4408 601C81B0
%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=14AF, count=0 -Traceback= 601C14FC
602000C8 60203958 601C4408 601C81B0
```

There is no workaround.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(33)CC

The caveat listed in this section is resolved in Cisco IOS Release 11.1(33)CC1:

- CSCdr36952

A Cisco router may reload or pause indefinitely when the IOS HTTP service is enabled and a browser connects to `http://<router-ip>/%%`. This may be exploited to produce a denial of service (DoS) attack.

Workaround 1: Disable the ip http server with the **no ip http server** command.

Workaround 2: Block port 80 connections to the router via access-lists or other firewall methods.

For further information, refer to the Security Advisory located at the following URL:

<http://www.cisco.com/warp/public/707/advisory.html>

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(32)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(33)CC. This section only describes severity 1 and 2 caveats:

- CSCdm29755

If two users on different tty connections simultaneously attempt to issue commands that access NVRAM (for example, issuing the **show startup-config** command), the router might reload. There is no workaround.

- CSCdp15392

A PA-4R-DTR port adapter may insert 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.

- CSCdk37522

RSP-based platforms running Cisco IOS Release 11.1 CC may stop passing outbound traffic on a PA-CT3/4T1 interface and display the following error message:

```
%RSP-3-RESTART: interface Serial<slot>/<bay>/<port>:<t1>, output stuck
```

There is no workaround.

- CSCdm11933

Transmit packets are dropped by the PA-CE3, the PA-CT3, and the PA-2CT3 under heavy bursty traffic when the outstanding transmit packets exceed the tx queue limit of an interface. There is no workaround.

- CSCdk30727

A Cisco 7000 series router running Release 11.1(20)CC (or later) might reset when executing the **show ip bgp regex** command over a large BGP table. There is no workaround.

- **CSCdm57759**
 A Cisco 7200 series router with an 8-port channelized E1 card running Cisco IOS Release 12.0(4)T might experience a memory leak in the small buffer pool.
 Workaround: Monitor the input/output (I/O) memory and reload the router when it is too low.
- **CSCdm69594**
 The interface delay metric is set inappropriately 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 usec. The delay for a port channel made up of one or more Gigabit Ethernets is 100 usec.
 This incorrect setting has implications for routing protocols that use interface delay as part of the metric, such as EIGRP, and may cause the routing protocol to prefer a route through a single interface over a route through a port channel, all else being equal.
 Workaround: Manually configure an appropriate delay under the port channel interface with the **delay x** command.
- **CSCdp36092**
 A VIP with two PA-A3-OC3MM port adapters running Cisco IOS Release 11.1(28.2)CC may pause for several minutes and display the following error messages:

```
%CBUS-3-CMDTIMEOUT: Cmd timed out, CCB 0x5800FF70, slot 5, cmd code 2 -Traceback=
60232F7C 60233488 6022BC30 60229F50 60153E10 60153FA0 60168788 60168774

%ATMPA-3-CMDFAIL: ATM5/0/0 Command Failed at ../src-rsp/rsp_vip_atmdx.c - line 354,
arg 32784 -Process= "Net Background", ipl= 2, pid= 42 -Traceback= 60297A34 60296948
60296A1C 6015A724 6015A914 601542F8 60168788 60168774
```

 After 5 to 10 minutes, the VIP reloads with the following error message:

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

 There is no workaround.
- **CSCdp55810**
 A Cisco 7200 series router running Cisco IOS Release 11.1(30)CC can hit a buffer leak in the small buffer pool. There is no workaround.
- **CSCdp74511**
 A Cisco 7507 router with a VIP2 ATM card running Cisco IOS Release 11.1(23)CC may experience a reload with a bus error at PC 0x600239BC, address 0x48. There is no workaround.
- **CSCdp88255**
 When CEF is disabled, either through configuration or due to an internal error, any interfaces that have the **ip verify unicast reverse-path** feature enabled will not forward any frames. This problem occurs on all platforms that support CEF and unicast RPF.
 Workaround: Re-enable CEF, or disable the unicast RPF feature from the interfaces using the **no ip verify unicast reverse-path** command

- CSCdp91476

The counters for conform and nonconforming packet and byte counts were only 32-bit in the MIB. As such, these could overflow in a very short time (matter of hours) when the traffic load was high. As part of resolving this DDTS, a 32-bit overflow counter has been added. This counter can be used in conjunction with the existing 32-bit counter to get the full 64-bit value.

In addition, a true 64-bit counter has also been added to the MIB.

SNMPv1 managers, or Cisco IOS Release 11.x are limited to using the 32-bit overflow counters. The 64-bit counters will be invisible to them.

However, SNMPv2c or SNMPv3 managers running on top of 12.x will be able to use either the 32-bit overflow counters, or simply the 64-bit counters.
- CSCdr06665

A Cisco 7200 series routers using an ATM CES port adapter will allocate memory and not release it when the **show controller** command is used while the ATM interface is administratively shut down. Eventually, the system may run out of memory and need to be reloaded. There is no workaround.
- CSCdr09895

Under heavy traffic, a PA-A3 port adapter might experience a SAR0 reload. If this condition occurs on a Cisco 7200 series router, you must reload the router to recover normal operation. On a Cisco 7500 series RSP, this situation might result in commands from the RSP to the port adapter failing, but the port adapter should be able to recover without a router reload. There is no workaround.
- CSCdm29580

A Cisco router configured with TCP header compression reloads with a bus error when Cisco Express Forwarding (CEF) is enabled.

Workaround: Disable TCP header compression before enabling CEF (reload may be required).
- CSCdp70710

When a Cisco 7500 series router has hundreds of Frame Relay point-to-point subinterfaces (a large scaled configuration) built on cT1s with subif and dlci logging messages disabled and snmp frame-relay trap enabled, then under the T1 line failure (or rather, line status change), the router could experience CPU hog and consequently Frame Relay links and circuits could fail to come up.

Workaround:

 - a. In global configuration mode, redirect the console logging messages to system buffers or a network host.
 - b. In interface configuration mode, where Frame Relay runs, disable subif and dlci logging messages by issuing the **no logging event subif-link-status** and **no logging event dlci-status-change** commands.
 - c. In global configuration mode, issue the **no snmp-server enable traps frame-relay** command. (SNMP-server enable frame-relay traps is disabled by default.)

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(31)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(32)CC. This section only describes severity 1 and 2 caveats:

- CSCdp33774
A VIP2 may reload within Nevada Error Interrupt Register.
Workaround: Increase the SRAM on the VIP2.
- CSCdp46465
Duplicate of CSCdp15196. A PA-H port adapter on a Cisco 7507 router reports an output rate of 54 Mbps when the actual line output speed is 45 Mbps (T3). There is no workaround.
- CSCdp52532
A Cisco 7200 series router with a PA-MC-4T1 installed may reload when you perform an SNMP query by running CiscoView. There is no workaround.
- CSCdp60859
On a PA-CT3 or a PA-CE3, when fixed tx threshold is used to enable or disable tx limiting, nonstressed channels may experience some transmit packet drops when one channel is under constant overstress traffic.
Workaround: Set the dynamic tx limit threshold according to the number of direct memory access (DMA) buffers in the VIP to ensure that there are tx buffers available for nonstressed channels.
- CSCdp24657
On a Cisco 7505 series router operating in an Open Shortest Path First (OSPF) multiaccess environment, when certain OSPF routes are deleted from the designated router, routing information between other OSPF routers is lost. There is no workaround.
- CSCdp49869
With VIP-based fair queuing and dCEF enabled, a Cisco router running Cisco IOS Release 11.1(29)CC1 experiences output packet drops on serial interfaces.
Workaround: Do not use VIP-based fair queuing.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(30)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(31)CC. This section only describes severity 1 and 2 caveats:

- CSCdm01124
Issuing **write** and **show configuration** commands at the same time from more than one vty on a high-end platform might cause the router to reboot if you are running software earlier than Release 12.0. There is no workaround.
- CSCdm44772
When two **show run** commands are issued simultaneously from two different vtys, one session may finish before the other. This may terminate a variable that still needs to be used by the other session and may cause a router reload.
Workaround: Do not issue simultaneous **show run** commands from two vtys.

- CSCdk79961
The driver (Ethernet) fails to count the frame check sequence (FCS) bytes when calculating the number of bytes transmitted or received on an Ethernet interface. Therefore, the octet count is always incorrect by a factor of four times the number of packets sent or received on the interface. There is no workaround.
- CSCdm79957
A Cisco 7507 router running Cisco IOS Release 11.1(26)CC may display incorrect data due to corrupted counters when an SNMP walk tool such as SNMX is executed on a serial interface to poll MIB data (for example, 1.3.6.1.2.1.2.2.1.10 if in Octets). There is no workaround.
- CSCdj45202
A new configuration command, **ip spd mode aggressive**, is available. When configured, all IP packets that fail sanity check, such as “bad checksum not version 4,” and “bad TTL,” will be dropped aggressively to guard against bad IP packets spoofing. The **show ip spd** command displays whether or not aggressive mode is enabled. Selective Packet Discard (SPD) random drop in RSP is supported.
When enabled, SPD works as follows:
 - When the **ip spd mode aggressive** command is issued, IP packets that fail sanity checks are classified as aggressive droppable packets.
 - When the IP input queue reaches the SPD minimum threshold (specified by **ip spd queue min-threshold n**), all aggressive droppable packets are dropped immediately while normal IP packets (not high-priority SPD packets) are dropped with increasing probability as the length of the IP input queue grows.
 - When the IP input queue reaches the SPD maximum threshold (specified by **ip spd queue max-threshold n**), all normal IP packets are dropped at 100 percent.
 - The default SPD minimum threshold is 10, while the default maximum threshold is 75.
 - To avoid an input interface that engages too many router resources, new packets (SPD or non-SPD) received from that interface are dropped when the interface has more than the input hold queue limit of input packets floating somewhere in the router.
- CSCdj18685
A reload is caused by a freed node 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 an Intermediate System to Intermediate System (IS-IS)-specific problem. There is no workaround.
- CSCdk77704
A Cisco 7200 series router experiences poor performance when fancy queuing such as weighted fair queuing or priority queuing is enabled on a Multichannel E1/T1 port adapter. There is no workaround.
- CSCdm84162
IP traffic on a Cisco 7200 series router fails when fast switching on a channelized T3 interface.
Workaround: Configure the CT3 interface with the **no ip route-cache** command.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(29)CC

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

- CSCdk90244

A Cisco 7200 series router might reboot when configured with Release 11.1(22)CC and Release 11.1(24)CC and IP CEF is enabled.

The Cisco router configured with Release 11.1(22)CC and IP CEF enabled came in a continuous reboot with an “Error Interrupt, PC 0x60249AC8” error message. The decoded stack points to memory corruption.

A Cisco router configured with Release 11.1(22)CC and IP CEF enabled, reboots with the following error message:

```
Software forced crash, PC 0x603005A8
```

The stack decoded points to memory corruption and the router reboots once every 12 hours. There is no workaround.

- CSCdm78036

A Cisco router running Cisco IOS Release 11.1(26)CC may hang with no log messages or other failure indication. The router remains unresponsive to console or other traffic that requires processing by the Route Switch Processor (RSP). There is no workaround.

- CSCdp03602

A Cisco 7507 router might reboot with the following error message:

```
fib_rp_process_mac_acc_stats, registry_case
```

There is no workaround.

- CSCdm18977

The PA-CE1 channel sometimes requires a **shutdown interface** or a **no shutdown interface** command to restore line protocol on Cisco IOS Release 11.1(24)CC. There is no workaround.

- CSCdm35733

FEBE line and path counters on a POS interface might not increment with the following images: rsp-jv-mz.111-18.CC.bin, rsp-jv-mz.111-24.CC.bin, and rsp-jsv-mz.120-3.0.2. There is no workaround.

- CSCdm53977

In OSPF, an area border router (ABR) will not create a type 3 link-state advertisement (LSA) from another area into area 0 for a link that is connected to the ABR in that other area.

Workaround: Use the **redistribute connected subnets** configuration command on the ABR. This will create a type-5 LSA.

- CSCdp02958

RSP4 platforms running Cisco IOS Release 11.1 CC might delete a loopback interface, along with the corresponding IBGP session configurations, from the system configuration. This causes the router to stop traffic forwarding.

Workaround: Put the configuration of the loopback interface and the related IBGP session into the router and reload.

- CSCdp09645
On Cisco 7000 family routers, a configuration containing several long as-path lists might force a reload in the regmatch software. There is no workaround.
- CSCdk68604
A PA-MC8T1 port adapter on a VIP card reloads with the following message:

```
%POT1E1-2-POT1E1FWCRASHED: POT1E1 F/W crashed: B - VIP reset
```


The VIP card resets and produces a crash file. All interfaces are lost. There is no workaround.
- CSCdk83363
The ATM Deluxe PA (PA-A3) SCR=0 port adapter might drop packets on PVCs with the sustainable cell rate (SCR) set to zero.
Workaround: Specify the SCR with a nonzero value.
- CSCdm58335
An MC-4T1 port adapter on a Cisco 7200 series router cannot establish ISDN layer 2 with an NTT ISDN central office switch after reloading or powering-on.
Workaround: Issue a **shutdown**, and then a **no shutdown** command on the T1 controller.
- CSCdm71880
A Cisco 7206 router with two Zytec power supplies can reload because of a power supply shutdown, even if all other devices connected to the same power supply do not experience any power failure. The voltage measured is always half of the normal amount. There is no workaround.
- CSCdm24286
A Cisco 7200 series router might become inaccessible because of a constant logging of the following message originating from LLC2 input:

```
SYS-2-LINKED: Bad enqueue of XXXXXXXX in queue YYYYYYYY.
```


There is no workaround.
- CSCdm37878
A Cisco 7000 series router with a Route Switch Protocol (RSP4) and VIP2 may reload due to memory corruption with an error message similar to the following:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x60638590 reading 0x60
```


There is no workaround.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(28)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(29)CC. This section only describes severity 1 and 2 caveats:

- CSCdm19573
A Cisco 7200 series router running Releases 11.1(22)CC or 11.1(25)CC with a PA-CT3 card configured for transparent bridging with local-area transport (LAT) enabled might not show LAT services when issuing the **show lat service** command on a serial interface. This happens even when the remote link, also using transparent bridging with LAT enabled, is advertising LAT services. There is no workaround.
- CSCdk41648
The Packet OC-3 Interface Processor (POSIP) on a Cisco 7500 series router might stop receiving packets. A common symptom is lines flapping, caused by keepalive loss. This condition is seen with VIP2-40s with POSIP hardware Revision 1.30.
Workaround: Configure the POSIP using the **microcode reload** command.
- CSCdm42165
On a Cisco 7513 router with a CT3IP card running Cisco IOS Release 11.1(23)CC, a single T1 channel may become locked up when a new T1 line is installed with a Cisco 3620 router at the other end. High-Level Data Link Control (HDLC) does not initialize after the Cisco 3620 router is brought up. When a **show interface** command is executed on the Cisco 7513 router, the “local loop” setting does not appear.
Workaround: Reload on the microcode and change to the following bring-up procedure:
 - a. Turn on the new T1 from end to end.
 - b. Issue a **no shutdown** command on the Cisco 7513 router interface.
- CSCdm71799
A Cisco 7206 router with an ATM uplink may reload when the ATM fiber connection is disconnected. There is no workaround.
- CSCdj18292
A Cisco router running Cisco IOS Release 11.1 CC fails to route a subnet directed broadcast as a 255.255.255.255 broadcast back out the same interface it received it from if the subnet is defined on that interface. There is no workaround.
- CSCdm28893
A Cisco router running Cisco IOS Release 11.1 (22)CC may reload with a bus error in OSPF while accessing dead memory. There is no workaround.
- CSCdm45233
On a Cisco 7200 series router running Cisco IOS Release 11.1(25)CC, dial-in users cannot connect via IP when fast switching is enabled.
Workaround: Use the **no ip route-cache** command to disable fast switching on all interfaces or use the **service disable-ip-fast-frag** to disable fast switching for IP fragments.

- 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.
- CSCdm67344
A Cisco router running an ATM-Lite PA line card on a VIP2-50 shows drops and spurious errors when distributed Cisco Express Forwarding (dCEF) is enabled.
Workaround: Turn off dCEF.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(27)CC

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

- CSCdm28550
When an ATM Lite port adapter interface receives an AAL5 packet of 65532 bytes, it creates a zero length packet internally and causes a VIP to reload. There is no workaround.
- CSCdm40249
A physical unit (PU) cannot be brought online after you configure a new Synchronous Data Link Control/data-link switching (SDLC/DLSW) pair.
Workaround: Reload the router.
- CSCdm51483
Using the **show ip igmp group** command may cause a bus error reload if an Internet Group Management Protocol (IGMP) entry is deleted during the execution of the **show ip igmp group** command. There is no workaround.
- CSCdm67167
A Cisco router might reload when you use a prefix-list with range entries in a route-map for default-origination. Range entries of a prefix-list are not meaningful in default-origination and are ignored in the checking match condition.
Work around: Use an access-list rather than a prefix-list in a route-map for default-origination. Another workaround is to avoid using range entries (for example, with “le/ge”) in such a prefix-list.
- CSCdm55716
An ATM subinterface might drop packets when distributed CEF (dCEF) is disabled. This problem only occurs on subinterfaces created after dCEF is on, and then is turned off.
Workaround: Enable, and then disable dCEF after creating a new subinterface.
- CSCdm64005
A PA-T3 port adapter may exhibit a timing problem resulting in dropped packets. There is no workaround.
- CSCdm71133
A Cisco router with ATM/LANE interfaces running IPX-EIGRP may have a **no ipx sap-incremental EIGRP** command automatically inserted into the running-config after a reload. This disables sap-incremental. There is no workaround.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(26)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(27)CC. This section only describes severity 1 and 2 caveats:

- CSCdk54265

When you upgrade to Release 11.1(20)CC, a significant change in the amount of time and CPU processor utilization is required to process a network management request. The processor is utilized 90–99% and utilization lasts for over one hour.

This condition exists when the demand poll (HP Open View in this case but it could also be netmon) walks the routing table through Simple Network Management Protocol (SNMP). This polling walks other things as well, such as Address Resolution Protocol (ARP) tables and interface descriptor blocks (IDBs), but these take less than ten seconds and have little effect on the processor.

The default priority of the SNMP process was changed from medium to low in Release 11.1, allowing the scheduler to service other processes while SNMP is polling. This change makes it rare that SNMP will interfere with normal routing functions of the router because packet forwarding and routing are medium- or high-level processes. SNMP relinquishes the processor if required. Conversely, SNMP uses all of the available processor to complete this task.

Workaround: Disable walking of the routing table using an SNMP view statement in the router configuration. This may hinder the discovery of unnumbered links in the network, as well as increase the time of discovery.

- CSCdm14098

A Cisco 7507 router reloads when entering the **show cdp entry** command. There is no workaround.

- CSCdk67183

T-line protocol does not come up on some of the T1 lines of a CT3. The following symptoms are seen:

- A T1 line comes up on both ends while the line protocol is down at both ends.
- No T1/T3 errors are seen on the controllers.
- When the **loop net line** command is entered on the serial interface on the CT3 side, the loop is seen successfully at the remote site.

Workaround: Reset the card or reload the microcode on the CT3IP card.

- CSCdk81576

When “network” statements are removed from the Open Shortest Path First (OSPF) configuration in a Cisco router, checks are not executed for overlapping networks. This results in the corresponding interfaces not enabling OSPF.

Workaround: Remove the overlapping “network” statement and reinsert it.

- CSCdm20127

On a Cisco 7000 series router running Cisco IOS Release 11.1(24)CC, a bus error at address 0xD0D0D19 is possible. There is no workaround.

- CSCdk60164

A Cisco 7505 router running Cisco IOS Release 11.1(21)CC1 gets errors on the console after Cisco Express Forwarding (CEF) is enabled. This occurs on several routers. If CEF remains enabled, the router will eventually hang and have to be rebooted. There is no workaround.

- CSCdm02157
When implementing the operation, administration, and maintenance (OAM) enhancement, the VIP2-50 and PA-A3 reload. There is no workaround.
- CSCdm05197
When IP CEF is turned off, ingress traffic for the Gigabit Ethernet Interface Processor (GEIP) under the ISL/Dot1Q subinterface becomes processor-switched. Only by turning on IP CEF can the switching path become fast switching (route cache) again. There is no workaround.
- CSCdm24099
An array overflow error in the PA-A3 periodic management code might cause memory corruption on a Cisco 7200 series router. This caveat was found under Release 11.1 CC, 12.0, 12.0 S, and 12.0 T. There is no workaround.
- CSCdm01617
A Cisco 7000 series router with several hundred data-link connection identifiers (DLCIs) cannot boot properly because of excessive console log messages related to the startup of Frame Relay PVCs. There is no workaround.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(25)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(26)CC. This section only describes severity 1 and 2 caveats:

- CSCdk54312
Online insertion and removal (OIR) on a Cisco 7500 series router running Cisco IOS Release 12.0 might cause “OUTPUT STUCK” and “CYBUS COMPLEX RESTARTS” messages. There is no workaround.
- CSCdk67709
Multilink PPP interleaving causes delay in outbound traffic on RSP platforms.
There is no workaround.
- 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 might 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 (for example, IBM SNA sessions may fail). There is no workaround.
- CSCdm05440
Selective Packet Discard (SPD) can erroneously discard “hello” packets from some routing protocols, such as OSPF, EIGRP, and HSRP. When a router is processing a lot of other packets at process level, the lost routing protocol packets can cause route and HSRP flapping, leading to intermittent data packet loss. There is no workaround.
- CSCdm06448
The PA-A2 port adapter CES part microcode download might fail during bootup. The port adapter becomes invisible to IOS.
Workaround: Reload the router.

- CSCdm10790
After a VIP or RSP reloads, all E1 controllers on PA-MC-8E1/120 modules continue to flap until the framing is toggled from NO-CRC4 to CRC4 and back again. This occurs with PA-MC-8E1/120 port adapters connected to customer premises equipment devices running framing NO-CRC4. It has been seen in Releases 11.1(21)CC, 11.1(23)CC, 11.1(24)CC, 12.0(2)XE1, and 12.0(3)T.
Workaround: Toggle the framing parameter on and off to stabilize the controller.
- CSCdm07023
Switched Multimegabit Data Service (SMDS) does not forward multicast traffic to the group address defined in the **smds multicast ip e19991112222** command as it did in all prior releases. In prior releases, it appended the command with **subnet subnetmask**. It now appends the command with **0.0.0.0 0.0.0.0** instead. The problem is that multicast traffic will no longer get forwarded to SMDS multicast addresses defined with the older **smds multicast ip e19991112222 subnet subnetmask** command.
This change causes routing protocols such as OSPF and EIGRP (which use multicast addresses to forward routing packets) to fail across the SMDS interface once users upgrade to newer code unless they manually change their configurations.
Workaround: Add the **smds multicast ip e19991112222 0.0.0.0 0.0.0.0** command under the SMDS interface to allow all multicast traffic to be sent out.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(24)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(25)CC. This section only describes severity 1 and 2 caveats:

- CSCdk83829
A router reload occurred in lab stress testing when the physical memory of the system was completely exhausted from huge numbers of routes and peers. There is no workaround.
- CSCdk81888
OSPF might reload if a corrupt protocol packet is received and the corruption is not detected through the IP checksum. Because the IP checksum detects most packet corruptions, a reload is highly unlikely unless a large percentage of OSPF packets are corrupt.
Workaround: Fix the source of the packet corruption, or shut down the link on which the incoming corrupt packets are received.
- CSCdk78845
When the prune-timers in the oil list are not identical, the mroute will still go to a “forwarding” status even when there is no listener. There is no workaround.

- CSCdj75305

This caveat (along with CSCdj75596) describes a symptom you might encounter with a VIP2-20 (VIP with 16 MB DRAM). You see a “malloc” error message for the slot where the VIP2-20 is installed the first time you enable Distributed Cisco Express Forwarding (dCEF) switching on the router or when the router is reloaded. This causes all VIP2-20s not to be able to perform dCEF switching. All packets that come into any interface on this VIP are sent to the RSP switched by CEF.

Workaround: Reenable VIP dCEF switching on this interface using the following commands:

```
Router> configure terminal
ip cef distributed switch
interface x/x/x
```

where all interfaces belong to this VIP

```
ip route-cache distributed
ip route-cache cef
end
```

Until this is fixed, dCEF will not work with VIP2-20s.

- CSCdk28971

The router does not handle TCP flows according to the weight defined by QoS after **reload** or **write memory/configure memory** commands. There is no workaround.

- CSCdk61320

When an encrypted kerberized Telnet is sent to a Cisco router, the initial setup goes fine, but garbage output results when packet decryption from the router occurs on the client side. When CEF is on, if an outgoing interface does not have CEF on (such as during SMDS encapsulation), packets are process-switched. This is due to a lack of IP cache creation. There is no workaround.

- CSCdk75670

A Cisco 7200 series router with a PA-MC-xT1 card might run out of I/O memory if one of the active T1 lines goes down suddenly. During the low I/O memory period, the router might stop forwarding packets through the interfaces on the card.

Workaround: Reload the router.

- CSCdk77016

A Cisco router using a tunnel with multicast traffic might experience a big buffer leak. There is no workaround.

- CSCdk80974

A Cisco 7513 router configured as a slave RSP with high system availability (HSA) crashes and halts. There is no workaround.

- CSCdk71109

When a router is running Cisco Express Forwarding (CEF) and an outgoing interface has CEF disabled (for example SMDS encapsulation), packets are process-switched because of the lack of an IP cache creation. There is no workaround.

- CSCdk72928

On a Cisco 7513 router running Release 11.1(20)CC with FDDI MAC accounting configured, a discrepancy exists between the CLI output and the SNMP walk output for CIP MacSwitched packets. The SNMP data is missing all output entries except those destined for ffff.ffff.ffff. There is no workaround.

- CSCdk74680
A Cisco 7206 router running Cisco IOS Release 11.1(22)CC reloads when `mgd_timer_set_exptime_internal()` is configured. There is no workaround.
- CSCdk82659
PA-MCE1 and PA-MCT1 port adapters may experience port flapping during conditions when the bandwidth of data being directed at the port adapter is greater than the physical bandwidth of the port adapter's interface when transmitting.
Workaround: Turn off the keepalives to reduce the amount of port flapping.
- CSCdk92886
Under heavy traffic loads when the network has extensive CEF entry tables to update, the router may experience GEIP reloads with `CMD_TIMEOUT` or "Block overrun" error messages on the console. The router will recover but there is traffic interruption. There is no workaround.
- CSCdk93443
The **clear cef linecard** command can cause CEF to be disabled on some slots. A microcode reload of the slot reenables CEF. There is no workaround.
- CSCdk88162
Packets are not padded correctly to Ethernet minimal frame size when the router forwards the packets out of the LANE interface. The problem is related to PA-A1 port adapter and Cisco IOS Release 11.1 CC.
Workaround: Turn off fast switching.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(23)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(24)CC. This section only describes severity 1 and 2 caveats:

- CSCdk40049
The Cisco 7200 series router has the following error message on startup:

```
%SYS-2-SUPNOT: Can't create Registry ISDN
```


There is no workaround.
- CSCdk79642
This bug was introduced by CSCdk34549 and only Release 11.1(24)CC is affected.
A reload might occur when both inbound route-map and inbound distribute-list/prefix-list filtering exist for a peer. There is no workaround.
- CSCdk34549
A slow memory leak is seen in the Cisco BGP router when it is running Release 11.2(14)P. There is no workaround.
- CSCdk74144
During low memory conditions (with the "MALLOCFAIL" message displayed), a Cisco 7200 series router might encounter a bus error condition at `msdp_native_forward` and 0x3c and reload. There is no workaround.

- CSCdk74808
When the IP unicast Reverse Path Forwarding (RPF) check is enabled on one subinterface, all the subinterfaces on that interface will have the check performed. This includes subinterfaces that were deleted. This situation may cause the router to drop packets that do not pass the reverse-path test. Note that this may only be an issue for asymmetric routes. There is no workaround.
- CSCdk22030
A Cisco 7505 router running Cisco IOS Release 11.1(19)CC1 cannot converge BGP after executing a **clear ip bgp** command. There is no workaround.
- CSCdk72452
When the ATM uplink is broken or the remote CES sees loss of signal or loss of frame, you need to generate an alarm to the local connected T1/E1 link. An alarm indication signal (all 1s) is sent to all of the time slots configured in the structured mode. There is no workaround.
- CSCdk69045
Custom queuing stops working completely as soon as the rate limit is activated and all queue counters are showing zero. It can be restored only by reloading the router. There is no workaround.
- CSCdk76192
Packets that have the “do not fragment” bit set do not generate an Internet Control Message Protocol (ICMP) unreachable packet when forwarded to an interface that requires fragmented packets. This behavior is observed only with dCEF switching mode in Cisco 7500 series routers. There is no workaround.
- CSCdk76520
The VIP2 reloads with the PA-MC-8E1/120 configured for vip_enable_tx_polling.
Workaround: Turn off keepalives at both ends of the link.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(22)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(23)CC. This section only describes severity 1 and 2 caveats:

- CSCdk57889
Occasionally, under extreme stress conditions, the PA-MC-T3 port adapter stops transmitting. There is no workaround.
- CSCdk58799
CiscoWorks is mistakenly represented by CT3IP when managing PA-MC-T3. There is no workaround.
- CSCdk63163
If the **ip pim send-rp-announce** command is configured when a router runs out of memory, the router might reload.
Workaround: Deconfigure this command if the router is known to be at risk for running out of memory.

- CSCdk19805

In the following scenario:

```
telnet1 telnet2 Host
rtr1
rtr2
```

If both Telnet sessions are encrypted and kerberized, the Telnet2 console might receive garbled characters. The commands entered in this session take effect on rtr2, but the output is illegible. There is no workaround.

- CSCdk23648

When multiple key distribution centers (KDCs) are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted.

The following are new kerberos commands:

- **kerberos timeout** <1-10>—Communications with the KDC use this timeout. The default value is five seconds.
- **kerberos retry** <1-5>—Communications with the KDC try this several times. The default value is four retries.

These commands show up in the configuration when not set to their default values. There is no workaround.

- CSCdk61689

Turning on permanent virtual circuit operation, administration, and management (PVC OAM) on the PA-A3 port adapter on a Cisco 7200 series router might cause a reload if there is an AAL5-NLPID PVC.

Workaround: Turn PVC OAM management off.

- CSCdk62487

When nondistributed CEF is enabled after multicast routing is enabled, multicast packets are dropped.

Workaround: Disable and enable multicast routing.

- CSCdk63661

A PA-A3 port adapter might stop receiving under stress with some cyclic redundancy check (CRC) errors on VCs.

Workaround: Clearing the interface restores the service.

- CSCdk65504

With distributed Cisco Express Forwarding (dCEF), the interface output counters might fail to be updated and the VIP console will display the following error message:

```
FIB-4-FIBXDRLN.
```

There is no workaround.

- CSCdk25121

The router goes down with a bus error and the following stack decode:

```
r4k_badpc_dummy ti1575_post_coalesce_rx ti1575_post_coalesce_fs c7100_cpu_pak_coalesce
ti1575_process_receive_packet atmces_1575_suni_interrupt atm_mux_mueslix
```

There is no workaround.

- CSCdk30791
CEF per-destination load sharing could be uneven. Under certain conditions, load distribution could be very skewed even when the network is very large and hashing source and destination addresses should give a fairly even distribution. There is no workaround.
- CSCdk44523
The PA-A3 port adapter does not support per interface fancy queuing (WFQ, CQ, PQ). There is no workaround.
- CSCdk47218
Configuring output rate-limiting with distributed CEF enabled on an interface that does not exist causes a system restart. There is no workaround.
- CSCdk47375
When you use a kerberized Telnet to communicate between two Cisco routers, the credentials might not be forwarded. There is no workaround.
- CSCdk50463
Frame Relay PVC accounting on point-to-point subinterfaces is incorrect with distributed Cisco Express Forwarding (dCEF) switching. There is no workaround.
- CSCdk59118
When using the OAM PVC management feature with PA-A1, the PVC cannot be re-created after manually removing a PVC that is down because of OAM failure.

Workaround: Do not manually remove a PVC when it is in the “OAM managed” down state. Wait for the OAM failure to clear, and then when the VC comes back up, remove and re-create it as usual.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(21)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(22)CC. This section only describes severity 1 and 2 caveats:

- 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 reboot. There is no workaround.
- CSCdj94991
When running Cisco IOS Release 11.1 CA, a VIP can reload with a software-forced reload and a traceback pointing to vip_pak_to_host_inline. This has been seen with a VIP2-based Packet-over-SONET Interface Processor (POSIP) although it potentially can occur with other interfaces.

Workaround: The Route Switch Processor (RSP) automatically recovers with a microcode reload.

- CSCdk10762

After a reboot or CBus complex restart, there is a small chance that one or more T1 lines in a CT3IP do not come back up properly. Specific symptoms for this failure are as follows:

The line comes up at both ends, no T1 alarms or performance-monitoring errors are 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, and the T1 number is 1–20 (T1 lines 21–28 are not affected by this problem).

A microcode reload is the only way the router will reload.

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 controller t3** command.

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

```
Router# show controller 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 an IOS image that includes firmware version 2.8.0 or later, the above display includes more hardware version details, as seen in these two examples:

```
Router# show controller 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 controller 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
```

Workaround: Hardware versions 5.0.0 and 5.0.255 are subject to this caveat. Hardware version 5.0.1 is not. (If you see a hardware version of 5 with no additional numbers, update your software to a more recent version.)

- CSCdk11206

The router reloads when ten or more standby groups are configured before the IP addresses. There is no workaround.

- CSCdk34128

When the router generates sufficient network traffic to saturate a serial interface on an M4T or M8T port 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.

- CSCdk25825

When hot swapping is performed (OIR) from one type of ATM card to another, the **show lane xxx** command might display incorrect LANE information. There is no workaround.

- CSCdk35821

Memory for crash context is freed when a VIP is removed, but an IF condition prevents it from being reallocated if a card is inserted. There is no workaround.

- CSCdk39920

When packets are bridged while the VC is torn down, incorrect VC values (zero) might be recorded in the bridge table entry. As a result, packets are dropped because the VC value gets set to zero before the subinterface is brought down.

Workaround: Remove the invalid bridge entry by executing the **clear bridge** command.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(20)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(21)CC. This section only describes severity 1 and 2 caveats:

- CSCdk36161
A VIP with multicast distributed switching (MDS) might reload after a **clear ip pim int count** command is issued.
Workaround: Do not use the **clear ip pim int count** command.
- CSCdj69424
When Cisco Express Forwarding (CEF) and fair queuing are configured on the same interface, the output packet and octet counters for the interface might be incorrect. This problem occurs because some packets are counted twice when congestion occurs.
Workaround: Disable fair queuing with the **no fair-queue** interface configuration command.
- CSCdk10713
Link Access Procedure, Balanced (LAPB) (and hence X.25) does not work over the CE3 interface; the line protocol stays down. There is no workaround.
- CSCdk10948
An incomplete CEF adjacency might be created on a Frame Relay multipoint subinterface configured with static address mapping. Slower switching performance over that interface occurs.
Workaround: Recycling the subinterface (that is, using a **shutdown** and **no shutdown** command sequence) might clear the problem.
- CSCdk02527
Currently, if the **ip flow-export source** command is specified in the configuration, it is not downloaded on to the VIP. As a result, the NetFlow UDP packets have 0.0.0.0 as the source IP address, which causes a problem for the NetFlow Collector.
Workaround: Temporarily remove the **ip flow-export source** command until this is resolved.
- CSCdk06571
If dCEF and Flow are enabled on an ATM interface that has QoS policy propagation enabled, the IP precedence of the packet is not rewritten.
Workarounds: Disable Flow, or run CEF.
- CSCdi74403
IPX data does not fast-switch packets over ISDN interfaces. There is no workaround.
- CSCdk06529
Stale TCP remote shell protocol (rsh) sessions do not terminate, and related processes stay in the process queue. Also, these paused processes seem to hold memory with obvious consequences and could be exploited in a denial of service attack.
Workaround: Clear the hung processes individually by using the **clear ip tcp tcb** command or a related option.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(19)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(20)CC. This section only describes severity 1 and 2 caveats:

- CSCdj88927
The router might reload with a bus error while changing encapsulation from PPP to HDLC on High Speed Serial Interfaces (HSSI) with high system availability (HSA). There is no workaround.
- CSCdk04126
The HSSI port adapter seems to hang intermittently, causing flaps.
Workaround: Reload the microcode on the router.
- CSCdj91037
Removing **router bgp** from the configuration might drive up CPU utilization, and might cause a “%SYS-3-CPUHOG in Process = Exec” message. Tracebacks showed that “bgp_reset_cache” led to “process_may_suspend_inline.” There is no workaround.
- CSCdj69073
When Cisco Express Forwarding (CEF) and fair queuing are configured on the same interface, the output packet and octet counters for the interface might be incorrect. This problem is caused by some packets getting counted twice when congestion occurs.
Workaround: Disable fair queuing with the **no fair-queue** interface configuration command.
- CSCdk07174
Routers configured to host Cisco Cache Engines using the Web Cache Control protocol (WCCP) will treat any host that sends them valid WCCP data as a Cache Engine, regardless of whether that host is actually a legitimate cache service provider. This can be exploited to divert HTTP traffic to unauthorized users. The WCCP protocol will be changed to provide better authentication.
Workaround: Use input access lists to prevent WCCP traffic sent by unauthorized hosts from reaching the router. WCCP uses UDP on port 2048.
- CSCdk09038
The router might reload or the VC might stop working if a VC is reconfigured while there is active traffic on the VC.
Workaround: Tear down the VC first, wait for a few seconds, and re-create the VC with new parameters if the traffic on the VC cannot be stopped.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(18)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(19)CC. This section only describes severity 1 and 2 caveats:

- CSCdj76595
Occasionally a Livingston PortMaster device broadcasts packets with their own MAC address but Token Ring bit order. This causes the Routing Information Identifier (RII) bit to be set in the source address, but there is no Routing Information Field (RIF). Because of that, the packet cannot be routed. It does not get discarded, and the input queue can accumulate packets.
Workaround: Remove the defective Livingston device from the network.
- CSCdj91100
The port-channel interface by default uses the MAC address of the first interface member of Fast EtherChannel. If the first interface member goes down, the port-channel changes its MAC address to the second interface member's MAC address. There is no workaround.

Resolved Caveats—Cisco IOS Release 11.1(1) Through 11.1(17)CC

All the caveats listed in this section are resolved in Cisco IOS Release 11.1(18)CC. This section only describes severity 1 and 2 caveats:

- CSCdj33812
A new configuration command now exists for RSP routers to control caching policies for memory regions. You can now configure the memory device (MEMD) to be accessed uncached by issuing the **memory cache-policy io uncached** configuration command.
This method is better than having to enter the **test rsp cache memd uncached EXEC** command every time the router is booted.
Workaround: Use this configuration command for problems like CSCdj52309 and CSCdj70296.
To restore the MEMD caching policy to the original write-through policy, use the **memory cache-policy io write-through** command. To determine what memory cache policies are currently configured on your router, use the **show rsp** command.
- CSCdj52309
A catastrophic problem has been identified that affects all Cisco 7500 series routers and Catalyst 5000 family switches. The problem occurs when you use packet tunneling in combination with certain timing conditions, packet sizes, and buffer usages. Affected images are being deferred and special images are being built.
Tunneling is being used as an abbreviation in this context to see a specific fast-switch to process-level code path traversed by translational bridging (TLB), source-route bridging (SRB), and remote source-route bridging (RSRB), and data link switching (DLSw).
When the packet tunneling logic on RSP- or RSM-equipped systems causes datagrams to be copied from SRAM to DRAM, an arithmetic error results in more bytes being copied than are remembered for clean-up processing. Reuses of the tunneling logic, in certain rare combinations of timing, packet sizes, and buffer usages, might result in those unaccounted bytes causing several anomalous system behaviors, including packet errors.
This software defect is exposed to all RSP and RSM images in the following Cisco IOS software releases: 11.2, 11.2 P, 11.2 BC, 11.3, and 11.3 T.

Solution: To eliminate the problems mentioned in the preceding section, we strongly recommend that you download and install one of the following Cisco IOS software release updates: 11.2(12a), 11.2(12a)P, 11.3(2a), or 11.3(2a)T.

Workarounds: CSCdj33812 provides a configuration command to avoid the software defect. This workaround is available in the following Cisco IOS Releases: 11.2(11.5), 11.2(11.5)P, 11.2(11.5)BC, 11.3(2.1), and 11.3(2.1)T. If you are using an earlier release, use the second workaround.

The two workarounds decrease performance to process-switching levels.

Workaround 1: CSCdj33812 incorporated a configurable command that will be stored in NVRAM.

Configure the router with the **memory cache-policy io uncached** command to work around CSCdj52309. To determine what memory cache policies are currently configured on your router, use the **show rsp** command.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# memory cache-policy io uncached
Router(config)# end
Router# show rsp
Throttle count 0, DCL timer count 0 active 0, configured 1 netint usec 4000,
netint mask usec 200 DCL spurious 0
Caching Strategies: Processor private memory: write-back Kernel memory view: uncached
IO (packet) memory: uncached Buffer header memory: uncached
```

To restore the MEMD caching policy to the original write-through policy, use the **memory cache-policy io write-through** command.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# memory cache-policy io write-through
Router(config)# end
Router# show rsp
Throttle count 0, DCL timer count 0 active 0, configured 1 netint usec 4000,
netint mask usec 200 DCL spurious 0 Caching Strategies: Processor private memory:
write-back Kernel memory view: write-back IO (packet) memory: write-through
Buffer header memory: uncached
```

Workaround 2: If operating with images that do not have CSCdj33812 support, use the following command:

```
Router# test rsp cache memd-fastswitch uncache
```

The above command must be entered after every reload.

Other considerations: Cisco IOS Releases 10.3, 11.0, and 11.1 major and ED releases are not exposed to CSCdj52309. Though these releases share the same arithmetic problem, the tunneling software is different, and there is no known or predicted combination of timing, packet sizes, and buffer usages that results in the same or different anomalous behaviors associated with Cisco IOS Releases 11.2, 11.2 P, 11.2 BC, 11.3, and 11.3 P. Cisco is using CSCdj52309 to repair the arithmetic problem in 10.3, 11.0, and 11.1 releases; however, no special images are being created because the anomalous behaviors are not present in those releases.

- CSCdj59639

In a rare timing situation, an Advanced Peer-to-Peer Networking/Dependent LU Requester (APPN/DLUR) router might reload because of a bus error/segV exception at ndr_sndtp_encap_mu. There is no workaround.

- CSCdi88756
A Token Ring Interface Processor (TRIP) interface configured for transparent bridging but not configured for source-route bridging might silently drop some incoming frames. Specifically, if the interface receives a frame with length less than 120 bytes and the Routing Information Identifier (RII) bit is set (indicating an SRB frame), it might drop the next frame received. This can cause the interface's keepalive processing to fail and can lead to sporadic resets on the interface. There is no workaround.
- CSCdj03047
You might see overrun or dropped messages on serial interfaces on a Fast Serial Interface Processor (FSIP) on a Cisco 7500 series router. The **showdown**, **no shutdown**, and **clear interface** commands do not clear this condition.

Workaround: Perform a command that causes a "Cbus complex" restart. For example, configure the MTU size to a different value, and then change it back to the proper configuration (the example below assumes the MTU was set to the default of 1500).


```
interface serial 1/0
mtu 8000
! to cause a cbus complex restart mtu 1500
! change back to the proper value
```
- CSCdj26511
A checkheaps reload on the VIP can occur with a Packet-over-SONET OC-3 Interface Processor (POSIP) when the line is flapping continuously. This occurs because the POSIP gets reset during line up/down events.

Workaround: Line flapping can be minimized by disabling keepalives or reloading one router at a time.
- CSCdj32533
If there is a **microcode reload** command in the configuration, and a FDDI Interface Processor (FIP) in the router, the router might have a problem while booting up. There is no workaround.
- CSCdj68602
The router functions correctly when only bridging is configured. If, while bridging is configured, you add an IP address to that interface and you attempt to send an IP ping on that interface, the CT3 reports a "bad vc message" and the link stops carrying traffic. The interface's inability to carry traffic is easily explained after many "bad vc" messages. The "bad vc" messages would appear to be some unpleasant interaction between bridging and IP. There is no workaround.
- CSCdj69939
If CRC32 is configured between two POSIPs with hardware revision 1.4 or earlier, upgrading one POSIP to hardware revision 1.5 or later might lead to packets that are 2 bytes too short or long, as reported by the **debug ip packet** command.

Workaround: Reload the router. One way to prevent this problem is to set CRC16 on both ends before upgrading the POSIP.

- CSCdj75983

On Fast Ethernet interfaces on Cisco 7500, Cisco 7200, Cisco 4000, or Cisco 3600 series routers, the regular Fast Ethernet port adapter **media-type** configuration command is missing the RJ-45 option; only the Media Independent Interface (MII) option is available.

For example, on a Cisco 7200 series router with a Fast Ethernet port adapter installed in slot 6/0, the problem looks like the following:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 6/0
Router(config-if)# media ?
MII Use MII connector <--- Only MII, no RJ45
```

Workaround: Configure the interface for RJ-45 using the **no media-type MII** command. For example, on a Cisco 7500 series router with a Fast Ethernet port adapter installed in slot 0/0/0, use the following configuration:

```
mintan-7500# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
mintan-7500(config)# interface fastethernet 0/0/0
mintan-7500(config-if)# no media MII <--- switch to RJ45
```

Platform defaults are correctly preserved for all platforms and images that default to RJ-45. The Cisco 3600 platform does not default to RJ-45 media for Fast Ethernet interfaces on Release 11.3 T only. The RJ-45 port on the Cisco 3600 series Fast Ethernet ports will not be usable in images with this problem.

This problem, CSCdj75983, starts to show up in the following releases:

Interim Release Maintenance Release: 11.1, 11.1(16.2), 11.1(17), 11.1 CA, 11.1(15.3)CA, 11.1(16)CA, 11.2, 11.2(10.4), 11.2(11), 11.2 P, 11.2(10.4)P, 11.2(11)P, 11.3, 11.3(1.2) N/A, 11.3 T, and 11.3(1.2)T N/A.

It is fixed within the following releases:

Interim Release Maintenance Release: 11.1, 11.1(17.1), 11.1(18), 11.1CA N/A, 11.1(17)CA, 11.2, 11.2(11.4), 11.2(12), 11.2 P, 11.2(11.4)P, 11.2(12)P, 11.3, 11.3(1.5), 11.3(2), 11.3 T, 11.3(1.5)T, and 11.3(2)T.

- CSCdj79497

When connecting FSIPs back-to-back in a DCE/DTC method, the router is acting as the DCE and provides a clock. The parser allows configuration of a clock up to 8 MB. Older FSIP hardware has a maximum throughput of 6.132 MB, and underruns or overruns can be seen if traffic exceeds that threshold.

Workaround: Clock for 4 MB, or use the PA-4T+ or PA-8T+ port adapters.

- CSCdj79992

Cisco 7200 series routers configured with Inter-Switch Link (ISL) on the C7200-I/O-FE Fast Ethernet port fail to transmit ISL encapsulated packets. There is no problem with native (non-ISL) packets going out on the same interface. This problem does not occur on the PA-FE-TX and PA-FE-FX port adapters, or when you run Cisco IOS Release 11.3(1) or 11.3(1)T.

Workaround: Use the PA-FE-TX or PA-FE-FX interfaces for ISL traffic or use Releases 11.3(1) or 11.3(1)T.

- CSCdj83777

With inbound route-map/distribute-list/sof-reconfig, some prefixes might be incorrectly denied. There is no workaround.

- CSCdj58132
A router reload might occur at the `isis_recursive_walk` routine. There is no workaround.
- CSCdj83578
This defect was caused by CSCdj71654: “ISIS: should not advertise parallel adjacencies in LSPs.” When two routers have parallel point-to-point adjacencies between them, a flap of such a parallel adjacency might not trigger a full shortest path first (SPF) run. As a result, the routing table is out of sync. There is no workaround.
- CSCdj79452
On a Cisco 7500 series router, the line protocol might come down if the T3 ports on a single VIP are configured for Kentrox mode (**dsu mode 1**) with different data service unit (DSU) bandwidth rates, whether you are using a two-port T3 card or two one-port T3 cards.
Workarounds (for Cisco 7500 series):
 - One single-port T3 card on a single VIP—The problem does not appear with this configuration.
 - Two single-port T3 cards on a single VIP—If you have a configuration where the two PA-T3 cards are configured for **dsu mode 1** (Kentrox DSU mode) with different rates (**dsu bandwidth**) on the same VIP, the possible workaround is to move one of the T3 cards to a different VIP.
 - One two-port T3 card on a VIP—If both the ports are configured for **dsu mode 1** (Kentrox DSU mode) with different rates (**dsu bandwidth**), the possible workaround is to configure only one of the ports for Kentrox mode.
 - Two two-port T3 cards on a VIP—If either of the two ports is configured for **dsu mode 1** (Kentrox DSU mode) with different rates (**dsu bandwidth**), the possible workaround is to move one of the T3 cards to a different VIP. If both ports are configured for Kentrox, the workaround is to move one port to a different VIP or configure a different DSU mode (because you can have only one Kentrox mode on this T3 card).

This problem appears only if either of the two T3 ports on a single VIP is configured for Kentrox mode with different rates (**dsu bandwidth**) or the same subrates.

Workaround: Configure the T3 ports for full rate.
- CSCdj23230
Under rare circumstances, a router reload might occur while you are running TCP to X.25 protocol translation. There is no workaround.
- CSCdj60905
The router reloads with an arithmetic exception. This problem is rare and observed in a context where a high usage of TCP encapsulation is configured, like DLSw or BGP. There is no workaround.
- CSCdj34203
An unexpected system reload at boot time might occur if there are ATM Interface Processor (AIP) cards enabled.
Workaround: Disable the AIP cards.
- CSCdj71438
SVCs can no longer be established when all existing ATM Interface Processors (AIPs) are extracted and hot swapped on a router.
Workaround: In the case of multiple AIPs, change them one at a time. In the case of only one AIP, insert a new AIP before extracting the existing AIP.

- CSCdj71597
A Cisco router might drop small LAN emulation (LANE) packets. There is no workaround.
- CSCdj76100
Data packets still go through a broadcast and unknown server (BUS) after a data VC is established. There is no workaround.
- CSCdj77846
When using AppleTalk Remote Access (ARA) Version 3.0, a Cisco router allocates an AppleTalk node address of 0, and PPP negotiation fails. There is no workaround.
- CSCdj79565
A VIP2 reloads and port adapters pause indefinitely and go into the administratively down state.
Workaround: Use the **no shutdown** command to bring the interfaces on the port adapters back up. The VIP crash does not seem to be always the same.
- CSCdj20995
The router reloads when it is being simultaneously configured on two separate terminal lines as follows:


```
tty1: conf t
      router ospf 1
tty2: conf t
      no router ospf 1
tty1: redist static subnet
```

 The reload occurs immediately after you enter the last command above. This applies to all routing protocols, not just OSPF. There is no workaround.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family. 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 72](#)
- [Platform-Specific Documents, page 72](#)
- [Feature Modules, page 73](#)
- [Cisco IOS Software Documentation Set, page 73](#)

Release-Specific Documents

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

- *Release Notes for Cisco IOS Release 11.1*

On CCO at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1

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

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

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

Platform-specific documents for the Cisco 7000 family routers are available 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 Cisco IOS Release 11.1 CC 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:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.1: Release Notes for Cisco IOS Release 11.1 CC and Features 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 CC 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. 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 9 lists the contents of the Cisco IOS Release 11.1 software documentation set, which is available in electronic form and in printed form if ordered.



Note

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.1

On the Documentation CD-ROM at:

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

Table 9 Cisco IOS Release 11.1 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> <i>Configuration Fundamentals Configuration Guide</i> <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
<ul style="list-style-type: none"> <i>Network Protocols Configuration Guide, Part 1</i> <i>Network Protocols Command Reference, Part 1</i> 	AppleTalk IP Addressing Novell IPX IP Routing Protocols
<ul style="list-style-type: none"> <i>Network Protocols Configuration Guide, Part 2</i> <i>Network Protocols Command Reference, Part 2</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

Table 9 Cisco IOS Release 11.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Networking Overview ATM DDR Frame Relay ISDN LANE SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	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"> • <i>Configuration Guide Master Index</i> • <i>Command Reference Master Index</i> 	

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
- 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.

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.

OpenSSL License:

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 71.

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.

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

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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].