



Text Part Number: 78-5275-09 Rev. B0

Release Notes for Cisco 7200 Series for Cisco IOS Release 11.3 AA

February 16, 2002

These release notes describe new features for the Cisco 7200 series routers that support Cisco IOS Release 11.3 AA, up to and including Cisco IOS Release 11.3(9)AA1 and 11.3(9)AA1a. Cisco IOS Release 11.3(9)AA1 is based on Cisco IOS Releases 11.3 and 11.3T. These release notes are updated with each maintenance release of the Cisco IOS software, which is typically every six weeks.

For a list of software caveats that apply to Release 11.3 AA, refer to the *Caveats for Cisco IOS Release 11.3 T* document and the “Important Notes and Caveats” section of the *Cross-Platform Release Notes for Cisco IOS Release 11.3*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the “Caveats” section on page 21.

Use these release notes with the cross-platform *Release Notes for Cisco IOS Release 11.3* and the *Release Notes for the Cisco 7000 Family for Cisco IOS Release 11.3 T* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Contents

This document includes the following sections:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 7
- Important Notes, page 15
- Caveats, page 21
- Related Documentation, page 28
- Service and Support, page 32
- Cisco Connection Online, page 33
- Documentation CD-ROM, page 34

Corporate Headquarters

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

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

Introduction

Cisco IOS Release 11.3(2)AA was the first release of these platform-specific release notes. For more information on the release policy for Cisco IOS Release 11.3 AA, see the *Cisco IOS Software Release 11.3AA* product bulletin #738 on CCO.

Cisco Systems provides several software releases based on a single version of Cisco IOS software. Maintenance releases provide solutions to software caveats. For more information about the Cisco IOS software release process, see the *Types of Cisco IOS Software Releases* product bulletin #537 located on CCO and the Documentation CD-ROM.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 11.3 AA, see the “New and Changed Information” section on page 7 and the “Related Documentation” section on page 28.

System Requirements

This section describes the system requirements for Release 11.3(9)AA1 and includes the following sections:

- Memory Requirements, page 2
- Hardware Supported, page 2
- Determining Your Software Release, page 3
- Updating to a New Software Release, page 3
- Feature Set Tables, page 3

Memory Requirements

Table 1 describes the memory requirements for Cisco 7200 series routers supported by Cisco IOS Release 11.3 AA.

Cisco 7200 series routers are shipped with a 16- or 20-MB Flash memory card.

Table 1 Memory Requirements for Cisco 7200 Series Routers

| Feature Sets | Image Name | Software Image | Required Flash Memory | Required DRAM Memory | Release 11.3 AA Runs From |
|----------------------------------|---------------------|----------------|-----------------------|----------------------|---------------------------|
| Enterprise Standard Feature Sets | Enterprise | c7200-js-mz | 16 MB Flash | 32 MB DRAM | RAM |
| | Enterprise/IPSec 56 | c7200-js56i-mz | 16 MB Flash | 32 MB DRAM | RAM |

Hardware Supported

Cisco IOS Release 11.3 AA supports the Cisco 7200 series:

- Cisco 7202
- Cisco 7204
- Cisco 7206

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

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 7200 series router, log in to the Cisco 7200 series router and enter the **show version EXEC** command. The following sample output from the **show version** command indicates the version number on the second output line:

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-MZ), Version 11.3(9)AA1, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Updating to a New Software Release

For information about upgrading to a new software release, refer to the *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification* product bulletin located on CCO.

From CCO, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click on **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**.

Feature Set Tables

Cisco IOS software is available in different feature sets depending on the hardware platform. Cisco 7200 series routers support only the Enterprise feature set in Cisco IOS Release 11.3 AA. Table 2 lists the features supported by the Enterprise feature set for Cisco 7200 series routers.

Note This feature set table contains only a selected list of features. This table is not a cumulative or complete list of all the features in each image.

Table 2 Cisco 7200 Series Enterprise Feature Set Features

| Feature | Enterprise Feature Set | IPSec |
|---|------------------------|-------|
| IBM Support | | |
| APPN High-Performance Routing | No | No |
| APPN MIB Enhancements | No | No |
| APPN over Ethernet LAN Emulation | No | No |
| APPN Scalability Enhancements | No | No |
| Bisync Enhancements, includes: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay | Yes | Yes |
| Cisco MultiPath Channel (CMPC) | No | No |
| Database Connection Feature | No | No |

Table 2 Cisco 7200 Series Enterprise Feature Set Features (continued)

| Feature | Enterprise Feature Set | IPSec |
|---|-------------------------------|--------------|
| DLSw+ Enhancements, includes: — Backup Peer Extensions for Encapsulation Types — DLSw+ Border Peer Caching — DLSw+ MIB Enhancements — DLSw+ SNA Type of Service — LLC2-to-SDLC Conversion between PU4 Devices — NetBIOS Dial-on-Demand Routing — UDP Unicast Enhancement | Yes | Yes |
| FRAS Enhancements, includes: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay | Yes | Yes |
| TN3270 LU Nailing | No | No |
| TN3270 Server Enhancements | No | No |
| Token Ring LANE | No | No |
| Tunneling of Asynchronous Security Protocols | Yes | Yes |
| Internet | | |
| DRP Server Agent | Yes | Yes |
| DRP Server Agent Enhancements | Yes | Yes |
| IP Routing | | |
| Easy IP (Phase 1) | Yes | Yes |
| Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations | Yes | Yes |
| IP Enhanced IGRP Route Authentication | Yes | Yes |
| TCP Enhancements, includes: — TCP Selective Acknowledgment — TCP Timestamp | Yes | Yes |
| LAN Support | | |
| AppleTalk Access List Enhancements | Yes | No |
| DECnet Accounting | Yes | No |
| IPX Named Access Lists | Yes | No |
| IPX SAP-after-RIP | Yes | No |
| NLSP Enhancements | Yes | No |
| NLSP Multicast Support | Yes | No |
| Management | | |
| Cisco Call History MIB Command Line Interface | No | No |
| Cisco IOS Internationalization | Yes | Yes |

Table 2 Cisco 7200 Series Enterprise Feature Set Features (continued)

| Feature | Enterprise Feature Set | IPSec |
|---|-------------------------------|--------------|
| Entity MIB, Phase 1 | Yes | Yes |
| SNMP Inform Requests/SNMP Manager | Yes | No |
| SNMPv2C | Yes | Yes |
| Virtual Profiles | Yes | Yes |
| Multimedia | | |
| IP Multicast Load Splitting Across Equal-Cost Paths | Yes | Yes |
| IP Multicast over ATM Point-to-Multipoint Virtual Circuits | Yes | Yes |
| IP Multicast over Token Ring LANs | Yes | Yes |
| PIM Version 2 | Yes | Yes |
| Stub IP Multicast Routing | Yes | Yes |
| Quality of Service | | |
| RTP Header Compression | Yes | Yes |
| Security | | |
| Double Authentication | Yes | Yes |
| Encrypted Kerberized Telnet | No | No |
| HTTP Security | Yes | Yes |
| Per-User Configuration | Yes | Yes |
| Reflexive Access Lists | Yes | Yes |
| TCP Intercept | Yes | No |
| Vendor-Proprietary RADIUS Attributes | Yes | Yes |
| Switching | | |
| AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs | Yes | No |
| CLNS and DECnet Fast Switching over PPP | Yes | No |
| DECnet/VINES/XNS over ISL, includes: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs | Yes | No |
| Fast-Switched Policy Routing | Yes | Yes |
| IPX Routing over ISL Virtual LANs | Yes | No |
| VIP Distributed Switching Support for IP Encapsulated in ISL | No | No |
| Terminal Services | | No |
| Virtual Templates for Protocol Translation | Yes | No |
| WAN Optimization | | |
| ATM MIB Enhancements | No | No |
| Enhanced ATM VC Configuration and Management | Yes | Yes |
| PAD Enhancements | Yes | No |

Table 2 Cisco 7200 Series Enterprise Feature Set Features (continued)

| Feature | Enterprise Feature Set | IPSec |
|--|------------------------|-------|
| PAD Subaddressing | Yes | No |
| WAN Services | | |
| Bandwidth Allocation Control Protocol | Yes | Yes |
| Dialer Watch | Yes | Yes |
| Enhanced Local Management Interface (ELMI) | Yes | Yes |
| Frame Relay Enhancements | Yes | Yes |
| Frame Relay MIB Extensions | Yes | Yes |
| Frame Relay Router ForeSight | Yes | Yes |
| ISDN Advice of Charge | No | No |
| ISDN Caller ID Callback | No | No |
| ISDN NFAS | Yes | No |
| Layer 2 Forwarding—Fast Switching | Yes | No |
| Leased Line ISDN at 128 kbps | No | No |
| MS Callback | Yes | Yes |
| PPP over ATM | Yes | No |
| Telnet Extensions for Dialout | No | No |
| X.25 Enhancements | Yes | Yes |
| X.25 on ISDN | No | No |
| X.25 Switching between PVCs and SVCs | Yes | Yes |
| X.28 Emulation | Yes | No |



Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to U.S. government export controls and have a limited distribution. Images to be installed outside the U.S. require an export license. Customer orders may be denied or subject to delay due to U.S. government regulations. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

New and Changed Information

The following sections list the new features supported by Cisco 7200 series routers in Cisco IOS Release 11.3 AA. For Release 11.3 AA and other features for Cisco products, refer to the specific product's release notes.

New Features in Release 11.3(9)AA1

There are no new features in Cisco IOS Release 11.3(9)AA1.

New Features in Release 11.3(9)AA

The following new feature is supported by Cisco 7200 series routers in Release 11.3(9)AA. For easy online access, the feature modules are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

VPDN Per User Config

The VPDN Per User Config feature sends the entire structured username to the AAA server the first time. This enables the Cisco IOS software to customize tunnel attributes for individual users using a common domain name or DNIS.

Previously, Cisco IOS sent only the domain name or DNIS to determine VPDN tunnel attribute information. Then, if no VPDN tunnel attributes were returned, Cisco IOS sent the entire username string. Because of this behavior, there is no way to define specific tunnel attributes for a particular user within a domain. It also limited the types of connections that are possible in a RADIUS Proxy VPDN roaming environment. All VPDN users are forwarded to the tunnel endpoint, even if they just need generic Internet access.

New Features in Release 11.3(8)AA

The following new features are supported by Cisco 7200 series routers in Release 11.3(8)AA. For easy online access, the feature descriptions are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

L2TP Optimal Fastswitching Support

L2TP Optimal Fastswitching Support is a user transparent performance enhancement that allows L2TP to have the same switching functionality as L2F (Layer2 Forwarding Protocol). This capability was added to L2F as part of the optimal fastswitching support for VPDN in Cisco IOS Release 11.3. This L2TP fastswitching support for LES (LAN emulation server) platforms, even on the LNS (L2TP Network Server), allows L2TP to scale to the large numbers of interfaces that L2F can support (1000+ sessions).

In this implementation, two route cache lookups used to forward a packet, one to switch to the virtual access interface and the other to switch from the virtual access interface to the output physical interface, have been reduced to one. This is accomplished by caching the complete IP/UDP/L2TP/PPP header, which is prepended to the packet that is to be tunneled, so that, when a packet is received on the input physical interface, the route cache lookup returns the output physical interface missing out the virtual interface. The cached header is then prepended to the packet and the appropriate reformatings are performed before the packet is switched as normal.

This feature is implemented in this way only for Cisco IOS Release 11.3 AA. In other releases, the scalability is provided by the FIB.

Configuring Key, Timeout, Retransmission per Radius Server

This security feature, also called, Per-Radius-server for key, timeout, and retransmit, adds per-server parameters to three global commands that apply to all RADIUS servers:

radius-server timeout m

radius-server retransmit n

radius-server key xyz

The parameters on a per-server basis define the “global” commands for each specified server. For example:

```
radius-server host 1.1.1.1 timeout n retransmit m key abc
radius-server host 2.2.2.2 timeout k retransmit 1 key def
```

If the user does not define the per-server value, a “global” commands value is used. Anytime the per-server options are used, they override the “global” value. If neither global, nor per-server values are defined, the defaults are used: timeout (5 seconds), retransmit (3 retries), and no key (respectively).

The **radius-server host** is specified by additional keywords of the three changed command syntax.

Configurable SLIPP/PPP Timeout Message

The Configurable SLIP/PPP timeout message is an enhancement to the exec login process whereby the prompt string can be set to some value that does not contain the prompt, thereby keeping the user scripts from becoming confused. When the username or password prompt times out, the prompt string is included as part of the timeout message. The presence of the prompt string in the timeout message can be confused with the login prompt by some scripts. A new command is added that can set the prompt string in the timeout message to a different value. Configurable SLIPP/PPP timeout message is related to the User-Configurable SLIP/PPP Banner with Parameter Insertion feature. For additional information about User-Configurable SLIP/PPP Banner with Parameter Insertion, see the following subsection.

User-Configurable SLIP/PPP Banner with Parameter Insertion

This User-Configurable SLIP/PPP Banner with Parameter Insertion feature is a compatibility enhancement that provides a Cisco IOS customizable SLIP command line parser for support of third party vendor equipment that is used to dial into a Cisco access router or server. This feature allows scripts designed to work with SLIP support on third party vendor equipment, such as Netcruiser negotiated parameters syntax, to negotiate compatibly when dialing into a Cisco access router or server.

Token Ring LAN Emulation Services

Token Ring LANE allows Token Ring LAN users to take advantage of ATM's benefits without modifying end-station hardware or software. ATM uses connection-oriented service with point-to-point signaling or multicast signaling between source and destination devices. However, Token Ring LANs use connectionless service. Messages are broadcast to all devices on the network. With Token Ring LANE, routers and switches emulate the connectionless service of a Token Ring LAN for the end stations.

By using Token Ring LANE, you can scale your networks to larger sizes while preserving your investment in LAN technology.

New Features in Release 11.3(7)AA

There are no new features in Release 11.3(7)AA.

New Features in Release 11.3(6)AA

The following new features are supported by Cisco 7200 series routers in Release 11.3(6)AA. For easy online access, the feature modules are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

DNIS Server Request Support in AAA

You can now authenticate users to a particular AAA server based on the session's Dialed Number Identification Service (DNIS) number. RADIUS directed-request now supports this capability.

Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS lets you know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems (Cisco 5200/5300) can receive the DNIS number. This functionality allows users to assign different RADIUS servers to different customers (that is, different RADIUS servers have different DNIS numbers).

Bundled in Cisco 7200 Series Routers

Channel Port Adapter (CPA) microcode xcpa26-2 has been bundled into Release 11.3(6)AA for the Cisco 7200 series routers. For more information, refer to the *Channel Port Adapter Microcode Release Note and Microcode Upgrade Requirements* located on CCO.

New Features in Release 11.3(5)AA

The following new features are supported by the Cisco 7200 series routers in Release 11.3(5)AA. For easy online access, the feature modules are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for access virtual private networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Show Caller

The **show caller** command is a network management feature that applies to dial protocols for public and private networks. It is a user interface command that displays information for incoming and outgoing connections. The **show caller** command supports ISDN and asynchronous modem connections and is supported for PPP, Multilink PPP, and SLIP. It also includes all NCPs running on PPP, including IP, IPX, and AppleTalk.

DNS Server Request Support in AAA

Microsoft Point-to-Point Protocol (PPP) clients have the ability to request either a primary or a secondary domain naming system (DNS) server from the network access server (NAS) during IP Control Protocol (IPCP) negotiation. To support this functionality using authentication, authorization, and accounting (AAA) security services, two new TACACS+ attribute-value (AV) pairs and two new vendor-proprietary RADIUS attributes have been added.

New Features in Release 11.3(4)AA

The following new features are supported by Cisco 7200 series routers in Release 11.3(4)AA. For easy online access, the feature modules are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

IETF-Compliant PPP over ATM

Point-to-Point Protocol (PPP) over Asynchronous Transfer Mode (ATM) is now available on an ATM-CES port adapter in a Cisco 7200 series router, thereby providing a significant increase in the number of PPP over ATM sessions per router.

In previous versions of PPP over ATM, you configured permanent virtual circuits (PVCs) for PPP over ATM on point-to-point subinterfaces. In this release, each PPP over ATM connection no longer requires two interfaces, a virtual access interface and an ATM subinterface. Instead, you can configure multiple PVCs for PPP over ATM on multipoint subinterfaces.

Also in this release, PPP over ATM is enhanced to support virtual circuit (VC) multiplexed encapsulation and complies with the Internet Engineering Task Force (IETF) draft on multiplexed encapsulation titled *PPP over AAL5 Internet Draft*. The previous version of PPP over ATM supported only frame forwarding data encapsulation (aal5ciscoPPP).

Note The IETF PPP over ATM feature does not currently support LLC encapsulated PPP over ATM adaptation layer 5 (AAL5).

ATM-CES Port Adapters

The ATM-CES port adapters (PA-A2-4T1C-OC3SM, PA-A2-4T1C-T3ATM, PA-A2-4E1XC-OC3SM, PA-A2-4E1XC-E3ATM, PA-A2-4E1YC-OC3SM, and PA-A2-4E1YC-E3ATM) are available on Cisco 7200 series routers. The ATM-CES has four T1 (1.544 Mbps) or four E1 (2.048 Mbps) ports (75- or 120-ohm) that can support both structured (N x 64 kbps) and unstructured ATM Forum-compliant circuit emulation services (CES), and one port that supports an OC-3 (155 Mbps) single-mode intermediate reach interface or a T3 (45 Mbps) or E3 (34 Mbps) standards-based ATM interface. The target application of the ATM-CES port adapter is access to a broadband public or private ATM network where multiservice consolidation of voice, video, and data traffic over a single ATM link is a requirement.

The ATM-CES port adapter supports the following features:

- Cross-connect Circuit Emulation Services (CES)—structured and unstructured
- Four -port T1 or E1 (75- or 120-ohm) constant bit rate (CBR)
- Network timing distribution
- On/off hook Channel Associated Signaling (CAS)
- Segmentation and reassembly (SAR) of up to 512 buffers simultaneously, where each buffer represents a packet
- Total of 2046 virtual circuits (VCs) of which up to 124 VCs can be CES VCs
- ATM Adaptation Layer (AAL) 5
- Single-port SONET/SDH OC-3 single-mode intermediate reach ATM uplink
- Single-port DS3/E3 ATM WAN uplink over T3/E3
- Traffic shaping
- Operation, Administration, and Maintenance (OAM) cells
- Online insertion and removal (OIR)
- Available Bit Rate (ABR)-ready hardware

The ATM-CES port adapters now support the following additional features:

- Available Bit Rate (ABR)—The ABR service category as specified in the ATM Forum Traffic Management Specification Version 4.0.
- Virtual Path Shaping—A virtual path (VP) is a logical association or bundle of virtual circuits (VCs).
- All traffic shaping features available with the **atm pvc** interface command are supported, and you can now configure the number of transmit channels for the interface with the **atm max-channels** interface configuration command.

In Release 11.3(2)T, the Enhanced ATM VC Configuration and Management feature set was introduced. The ATM-CES port adapters support the Enhanced ATM VC Configuration and Management feature, which includes new and enhanced capabilities that allow you to create and manage ATM PVCs and SVCs with more ease and improved integrity. This feature set includes the following features:

- **New VC Configuration**—Allows you to create ATM permanent virtual circuits (PVCs), switched virtual circuits (SVCs), static maps, and associated virtual circuit (VC) parameters more easily and with fewer errors using new ATM commands in new VC command modes.
- **VC Integrity Management**—Allows you to manage your ATM PVCs and SVCs so that your router receives immediate notification of when these VCs go down in your network. Upon notification, protocols can reroute packets and prevent unpredictable and relatively long time out periods.
- **PVC Discovery**—Allows you to enable your router to automatically assign (or discover) PVCs on an ATM interface or subinterface using information from an attached adjacent switch.
- **Multiprotocol Inverse ARP**—Allows you to enable a dynamic protocol mapping between an ATM PVC and a network address by configuring Inverse Address Resolution Protocol (Inverse ARP) on ATM PVCs running IP or IPX.
- **Rate Queue Tolerance**—Allows you to configure a range of peak rates on a single rate queue, thereby improving ATM rate queue usage.

For additional information, refer to the *PA-A2 ATM CES Port Adapter Installation and Configuration* publication that accompanies the hardware.

Cisco 7202 Router

The Cisco 7202 is the newest member of Cisco 7200 series routers, which consist of the 2-slot Cisco 7202, 4-slot Cisco 7204, and the 6-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, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN), and serial media.

Network interfaces reside on port adapters that provide the connection between the router's Peripheral Component Interconnect (PCI) 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 install the port adapters in either of the two available port adapter 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)—Allows you to add, replace, or remove port adapters without interrupting the system or entering any console commands.
- Dual hot-swappable, load-sharing power supplies—Provide system power redundancy; if one power supply or power source fails, the other power supply maintains system power without interruption. 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—Allow you to maintain normal system operation by resolving adverse environmental conditions before any loss of operation.
- Downloadable software—Allows you to load new images into Flash memory remotely, without having to physically access the Cisco 7202 router for fast, reliable upgrades.

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

New Features in Release 11.3(3)AA

There are no new features for the Cisco 7200 series routers in Release 11.3(3)AA.

New Features in Release 11.3(2)AA

The following new features are supported by the Cisco 7200 series routers in Release 11.3(2)AA. For easy online access, the feature modules are linked to the applicable Cisco IOS feature module if one exists. Click on the link to open the feature module.

Scalability

The number of physical and logical interfaces supported on Cisco 7200 series routers has been increased to 3000. This increase allows Cisco 7200 series routers to support applications like virtual private dial-up network (VPDN) and WAN aggregation, where Cisco 7200 series routers must handle a large number of interfaces. VPDN allows the forwarding of Point-to-Point Protocol (PPP) links from an Internet service provider (ISP) to a home gateway.

Cisco IOS File System

The Cisco IOS file system (IFS) feature provides a single interface to all file systems the router uses:

- Flash memory file systems
- Network file systems (TFTP, rcp, FTP)
- Any other endpoint for reading or writing data (NVRAM, the running configuration, ROM, raw system memory, system bundled microcode, Xmodem, Flash load helper log, LAN Extender interfaces, modems, and BRI MUX interfaces).

Conditionally Triggered Debugging

The conditionally triggered debugging feature limits debugging messages based on their related interface or subinterface. When this feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface. However, the router does not generate debugging output for packets entering or leaving through a different interface. This feature allows you to focus debugging output on the problematic interface or interfaces. You can specify the interfaces explicitly. For example, you may only want to see debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet specified conditions, such as a particular username, calling party number, or called party number. If you specify multiple conditions, the interface must meet at least one of the conditions.

AAA Scalability

The authentication, authorization, and accounting (AAA) scalability feature allows you to configure and monitor the number of background processes allocated by the PPP manager in the network access server (NAS) to deal with AAA authentication and authorization requests. In previous Cisco IOS releases, only one background process was allocated to handle all AAA requests for PPP. This meant that parallelism in AAA servers could not be fully exploited. The AAA Scalability feature lets you configure the number of processes used to handle AAA requests for PPP, thus increasing the number of users that can be simultaneously authenticated or authorized.

OSPF LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group together Open Shortest Path First (OSPF) link state advertisements (LSAs) and pace the refreshing, checksumming, and aging functions. The group pacing results in more efficient use of the router.

OSPF Point-to-Multipoint Networks with Neighbors

OSPF has two new features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks.

- On point-to-multipoint broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the **neighbor** command, in which case you should specify a cost to that neighbor.
- On point-to-multipoint nonbroadcast networks, you now use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Before this feature, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the **neighbor** command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hellos, updates, and acknowledgments were sent using multicast. In particular, multicast hellos discovered all neighbors dynamically. If you were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), the routers could not dynamically discover neighbors. This feature allows the **neighbor** command to be used on point-to-multipoint interfaces. On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumes that the cost to each neighbor is equal. The cost is configured with the **ip ospf cost** command. In reality, the bandwidth to each neighbor is different, so the cost should be different. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

Important Notes

The following sections contain important notes about Cisco IOS Release 11.3 AA and can apply to Cisco 7200 series routers.

Cisco IOS Release 11.3 AA End of Sales and End of Engineering

End of Engineering (EOE) means there are no more regularly scheduled maintenance releases. The last maintenance release scheduled on the EOE date is only available through CCO and Field Service Operations—not through manufacturing.

- Cisco IOS Release 11.3 AA is scheduled to reach End of Sales (EOS) status with maintenance Releases 11.3(9)AA on Cisco 7200 series routers.
- Release 11.3 AA is scheduled to reach EOE with Release 11.3(9)AA.

For the most up-to-date information on the status of EOS or EOE, refer to the *Cisco IOS Software Release 11.3AA End of Sales and End of Engineering Milestones* product bulletins located on CCO.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under Cisco IOS 11.3, click on Cisco IOS Software 11.3AA End of Sales and Engineering (#820: 11/98)

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that will need to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were “restarted by power-on”, even when that is not the case.

Customers should assume that any potential attacker is likely to know that the existence of this vulnerability and the ways to exploit it. An attacker can use tools available to the public on the Internet. An attacker does not need to write any software to exploit the vulnerability. Minimal skill is required. No special equipment is required.

Despite Cisco’s specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this vulnerability.

This vulnerability notice was posted on Cisco’s World Wide Web site:

<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>

This information was also sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 2 of *Software Versions and Fixes*. Affected versions include 11.3AA, 11.3DB, and all 12.0 versions (including 12.0 mainline, 12.0S, 12.0T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 2. Cisco is correcting the vulnerability in certain special releases and will correct it in future maintenance and interim releases. See *Software Versions and Fixes* for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic using access lists. See “Workarounds” for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have already configured protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System Software”. Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800,ubr900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the ubr7200), 7500, and 12000 series,
- Most recent versions of the LS1010 ATM switch,
- Some versions of the Catalyst 2900XL LAN switch,
- Cisco DistributedDirector.

Affected software versions, which are relatively new, are not necessarily available on every device listed above.

If you are not running Cisco IOS software, you are not affected by this vulnerability. The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series) are not affected.
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines are not affected.
- MGX (formerly known as the AXIS shelf) is not affected.

- Host-based software is not affected.
- Cisco PIX Firewall is not affected.
- Cisco LocalDirector is not affected.
- Cisco Cache Engine is not affected.

This vulnerability has been assigned Cisco DDTS Caveat ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers, regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 2 gives Cisco's projected fix dates.

Make sure your hardware had adequate RAM to support the new software before installing it. Amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2(11)P to 11.2(17)P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be made available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

<http://www.cisco.com>

Customers with service contracts should obtain new software through their regular update channels (generally via Cisco's World Wide Web site). They may upgrade to any software release, but they must remain within the boundaries of the feature sets they have purchased.

Customers without service contracts may upgrade to obtain only the bug fixes; they are not offered upgrades to versions newer than required to resolve the defects. In general, these customers will be restricted to upgrading within a single row of Table 2 below, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence of your entitlement to a free update. Free updates for non-contract customers must be requested through the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, that list should be applied to all interfaces to which attackers may be able to send datagrams. Interfaces include not only physical LAN and WAN interfaces, but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and/or interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts; only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this vulnerability.

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets might be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution, especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of 12.0 mainline software is 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running 12.0(2), and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to 12.0(2a). Release 12.0(2a) is a “code branch” from the 12.0(2) base, which will merge back into the 12.0 mainline at 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from 12.0(2a) is to 12.0(3).

Table 2 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 3 Affected and Repaired Software Versions

| Cisco IOS Major Release | Description | Special Fix ¹ | First Fixed Interim Release ² | Fixed Maintenance Release ³ |
|--|---|-------------------------------------|--|--|
| Unaffected Releases | | | | |
| 11.2 and earlier—all variants | Unaffected early releases (no syslog server) | Unaffected | Unaffected | Unaffected |
| 11.3, 11.3T, 11.3DA, 11.3MA, 11.3NA, 11.3WA, 11.3(2)XA | 11.3 releases without syslog servers | Unaffected | Unaffected | Unaffected |
| Releases based on 11.3 | | | | |
| 11.3AA | 11.3 early deployment for AS58xx | 11.3(7)AA2, 8-JAN-1999 ⁴ | 11.3(7.2)AA | 11.3(8)AA, 15-FEB-1999 |
| 11.3DB | 11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM | | | 11.3(7)DB2, 18-JAN-1999 |
| Releases based on 12.0 | | | | |
| 12.0 | 12.0 Mainline | 12.0(2a), 8-JAN-1999 | 12.0(2.4) | 12.0(3), 1-FEB-1999 |
| 12.0T | 12.0 new technology early deployment | 12.0(2a)T1, 11-JAN-1999 | 12.0(2.4)T | 12.0(3)T, 15-FEB-1999 |
| 12.0S | ISP support; 7200, RSP, GSR | | 12.0(2.3)S, 27-DEC-1998 | 12.0(2)S ⁵ , 18-JAN-1999 |
| 12.0DB | 12.0 for Cisco 6400 universal access concentrator node switch processor (lab use) | | | 12.0(2)DB, 18-JAN-1999 |

Important Notes

Table 3 Affected and Repaired Software Versions (continued)

| Cisco IOS Major Release | Description | Special Fix¹ | First Fixed Interim Release² | Fixed Maintenance Release³ |
|--------------------------------|---|---|--|--|
| 12.0(1)W | 12.0 for Catalyst 8500 and LS1010 | 12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only) | 12.0(1)W5(5.15) | 12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7)) |
| 12.0(0.6)W5 | One-time early deployment for CH-OC12 module in Catalyst 8500 series switches. | Unaffected; one-time release | Unaffected | Unaffected; general upgrade path is via 12.0(1)W5 releases. |
| 12.0(1)XA3 | Short-life release; merged to 12/0T at 12.0(2)T | Obsolete | Merged | Upgrade to 12.0(2a)T1 and/or to 12.0(3)T. |
| 12.0(1)XB | Short-life release for Cisco 800 series; merged to 12.0T and 12.0(3)T | 12.0(1)XB1 | Merged | Upgrade to 12.0(3)T. |
| 12.0(2)XC | Short-life release for new features in Cisco 2600, Cisco 3600, ubr7200, ubr900 series; merged to 12.0T at 12.0(3)T. | 12.0(2)XC1, 7-JAN-1999 | Merged | Upgrade to 12.0(3)T |
| 12.0(2)XD | Short-life release for ISDN voice features; merged to 12.0T at 12.0(3)T. | 12.0(2)XD1, 18-JAN-1999 | Merged | Upgrade to 12.0(3)T |
| 12.0(1)XE | Short-life release | 12.0(2)XE, 18-JAN-1999 | Merged | Upgrade to 12.0(3)T |

1 A special fix is a one-time release that provides the most stable immediate upgrade path.

2 Interim releases are tested less rigorously than regular, maintenance releases; interim releases may contain serious bugs.

3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.

4 All dates in this table are estimates, subject to change.

5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release in which the vulnerability is fixed.

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. This section contains open and resolved caveats only for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 11.3 and Cisco IOS Release 11.3 T are also in Cisco IOS Release 11.3 AA.

For information on caveats in Cisco IOS Release 11.3, refer to the “Important Notes and Caveats for Release 11.3” section in the cross-platform *Release Notes for Cisco IOS Release 11.3* document which is located on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* document which is located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Caveats for Release 11.3(1)AA Through 11.3(9)AA1 and 11.3(9)AA1a.

This section describes possibly unexpected behavior by Release 11.3(9)AA1 and 11.3(9)AA1a.. Unless otherwise noted, these caveats apply to all 11.3 AA releases up to and including 11.3(9)AA1 and 11.3(9)AA1a.

- 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>

Basic System Services

- CSCdk51178

The "disconnect-cause" and "disconnect-cause-ext" attributes are missing in the TACACS+ network accounting stop record. There is no workaround.

Interfaces and Bridging

- CSCdm17766

ISDN Layer 2 will not initialize when High-Level Data Link Control (HDLC) and STAC Compression are combined.

Workaround: Run Cisco IOS Release 11.3(8.3)AA or disable STAC Compression.

Wide-Area Networking

- CSCdk75741
The **PPP timeout idle** command under the virtual template interface is not operating properly for PPP over ATM and PPP over Frame Relay.
Idle timers fail to reset when NCP traffic leaves the Virtual Access Interface, causing the PPP link to be dropped after the timeout although the link is not idle.
- CSCdk80734
The router might reload when the X.25 over TCP (XOT) task attempts to exit, which is programmed to occur after 60 seconds of idleness.
Workaround: Avoid using XOT or ensure that XOT never goes idle.
- CSCdk89688
When running Multilink PPP with Cisco IOS Release 11.3(7)AA1, the router might reload with a "restarted by bus error at PC 0x60AC49A8 address 0x0" message.
There is no known workaround.
- CSCdm05164
A multihop L2TP tunnel does not tear down all hops when cleared or refused at the multihop L2TP network server (LNS).
Workaround: Avoid clearing, through the CLI, a multihop tunnel from the LNS.
- CSCdm05357
On a deployment which is not Cisco to Cisco, L2TP pauses indefinitely when parsing an invalid control message with a zero-length attribute value pair (AVP).
There is no known workaround.
- CSCdm18137
On Cisco routers running Cisco IOS Release 11.3(8)AA1, connections might experience unexpected PPP LCP Timeouts.
There is no known workaround.
- CSCdm19619
Point to Point Protocol(PPP) reverts to the authenticating phase when Virtual Private Dial-up Networking (VPDN) authorization fails.
There is no known workaround.

Caveats for Release 11.3(1)AA Through 11.3(8)AA

This section describes possibly unexpected behavior by Release 11.3(8)AA. Unless otherwise noted, these caveats apply to all 11.3 AA releases up to and including 11.3(8)AA.

IP Routing Protocols

- CSCdk75249
On a Cisco 7200 series router, removing a secondary IP address from a Fast Ethernet (FE) interface with more than 250 secondary addresses mapped to more than 4000 IP addresses might consume 100% of the central processing unit (cpu) for 10 minutes.
Workaround: Do not remove the secondary IP address during high-traffic periods.

Miscellaneous

- CSCdk50386
The **show syscon mibpoll** command displays no data if the community strings on the system controller manager and the system controller agent are different.
Workaround: Make the strings on the system controller manager and the system controller agent identical.
- CSCdk86801
Conditional debugging called does not trigger debugs when the number is called.

Caveats for Release 11.3(1)AA Through 11.3(7)AA

This section describes possibly unexpected behavior by Release 11.3(7)AA. Unless otherwise noted, these caveats apply to all 11.3 AA releases up to and including 11.3(7)AA.

Wide-Area Networking

- CSCdk62966
Excessive numbers of L2TP tunnels on a Cisco 7206 router with an NPE-200 processor will cause the CPU to overload and cause a reload. There is no workaround.
- CSCdk66751
An L2F home gateway displays incorrect output counters for both the individual sessions and the tunnel for any session that has an IP cache entry. However, the interface counters are correct. There is no workaround.

Caveats for Release 11.3(1)AA Through 11.3(6)AA

This section describes possibly unexpected behavior by Release 11.3(6)AA. Unless otherwise noted, these caveats apply to all 11.3 AA releases up to and including 11.3(6)AA. For additional caveats applicable to Release 11.3(6)AA, see the caveats sections for newer 11.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.3(7)AA.

EXEC and Configuration Parser

- CSCdk52457

Using Ctrl-x to terminate a Telnet connection might cause the router to reload. There is no workaround.

IP Routing Protocols

- CSCdk47229

A Cisco router reloads within 25 minutes if you have a demand circuit (including a virtual link) and external LSA's on a router.

Workaround: Do not to use a demand circuit with virtual links.

Caveats for Release 11.3(1)AA Through 11.3(5)AA

This section describes possibly unexpected behavior by Release 11.3(5)AA. Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(5)AA.

All the caveats listed in this section are resolved in Release 11.3(6)AA.

Wide-Area Networking

- CSCdk26814

Signaling occurs when an event such as changing the MTU size or clearing the ATM interface generates a media_hw_reset. ATM SVC applications such as LANE or static map refuse to create an SVC because they think it still exists.

Workaround: Use **shutdown interface/no shutdown** interface commands to clear all state information at the signalling layer.

Miscellaneous

- CSCdk48652

Issuing the command **ping docsis** from a Telnet session after increasing the number of vty lines might cause the system to reboot.

Workarounds: Reload the system after changing the number of vty lines, or do not issue the **ping docsis** command from a Telnet session.

- CSCdk08256

This is a continuation of CSCdj87212. The customer is running Release 11.1(18.2)CA as a fix for CSCdj87212 and the following messages show in the log:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=60CE15D8, count=0 -Traceback=
601D633C 60168750 601688BC 601DCC94 60712C84 60713128 607105AC 60710 BC4 60710220
601F0FB0 601F0F9C
```

The cause was due to misplacement of the packet header in the transparent bridging path.

We added more protection at the driver level to prevent this error in the future. See CSCdk26015.

- CSCdk38476

RADIUS accounting does not work if you have separate authentication and accounting servers. There is no workaround.

- CSCdk49535

A rare event was detected that caused the Cisco uBR to reboot when deleting a cable modem. This fix adds protection to the uBR software against such conditions, solving the rebooting problem. No known workaround exists for this problem.

Caveats for Release 11.3(1)AA Through 11.3(4)AA

This section describes possibly unexpected behavior by Release 11.3(4)AA. Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(4)AA.

All the caveats listed in this section are resolved in Release 11.3(5)AA.

Basic System Services

- CSCdj91329

The command **show ip bgp** causes the router to reload when routes are displayed.

- CSCdk20606

The “tty daemon” process might use a large percentage of the available CPU if large amounts of data are sent to an asynchronous port over a Telnet connection (port 20xx, 60xx, and so on). Historically, the workaround has been to use a TCP stream mode connection instead (port 40xx, for example), but new features like fax dialout require the Telnet protocol for proper operation and to send large amounts of data.

Miscellaneous

- CSCdk23648

There is no way to control time out so that failover can occur when multiple KDCs are configured. This causes common client applications to fail before the next KDC is contacted.

There is no workaround.

Caveats for Release 11.3(1)AA Through 11.3(3)AA

This section describes possibly unexpected behavior by Release 11.3(3)AA. Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(3)AA. For additional caveats applicable to Release 11.3(3)AA, see the caveats sections for newer 11.3 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.3(4)AA.

Wide-Area Networking

- CSCdj91389

Configuring a line for **autoselect** without also configuring **autoselect during-login** might cause the router to pause indefinitely or reload. If **debug modem** is enabled, you will see type 0 timer expiration messages appearing continuously.

Caveats for Release 11.3(1)AA Through 11.3(2)AA

This section describes possibly unexpected behavior by Release 11.3(2)AA. Unless otherwise noted, these caveats apply to all 11.3 AA releases up to and including 11.3(2)AA.

All the caveats listed in this section are resolved in 11.3(3)AA.

Basic System Services

- CSCdj64910

An unconfigured system might send an inappropriate number of bootp requests after powerup in an attempt to find a usable IP address for autoconfigure. On a system with very large numbers of interfaces (for example, ISDN PRI or channelized interface), a CPUHOG error might occur.

- CSCdj74094

Packets are not classified to the correct conversation or precedence with Weighted Fair Queueing (WFQ) and Weighted Random Early Detection (WRED). This occurs only for IP netflow and optimum switching. The workaround is to disable optimum switching (in Cisco IOS feature sets identified by -p-) and enable netflow switching.

IBM Connectivity

- CSCdj83835

FRAS-Host Passthru does not work when **dlsw local-peer** is configured.

Workaround: Disable **dlsw local-peer** or configure **fras-host dlsw-local-ack**.

- CSCdj84579

During session setup from an end node to a logical unit on a low-entry networking node (LEN) served by VTAM, the session setup can fail. In Release 11.3 the following message is seen on the failing node:

```
%APPN-3-logdsDS_NEWDS1fa_LOGMSG_04: DS - FSM(NNSolu): invalid input value = 8x
%APPN-3-logdsDS_NEWDS1fa_LOGMSG_05: DS - FSM(NNSolu): state error, lcb: 8x
pcid: 8x8x row: 1632511552 col: -715957806 inp: 8x
```

This caveat affects Release 11.3 only.

- CSCdj84659

APPN/DLUR: A router reload can occur when DLUR processes a flow on the DLUS/DLUR connect that must be responded to negatively because the physical unit (PU) has disconnected. This is a regression defect introduced by CSCdj59639.

- CSCdj87903

The APPN network node was enhanced to time out locate searches that were pending for more than 9 minutes. If another node was not responding to locates, a significant amount of memory could be allocated to the network node while it waited on responses to the outstanding locates. This could result in memory shortages in some cases.

Interfaces and Bridging

- CSCdj84628

The POSIP interface might receive and switch packets even when it is in the administrative down state. This has been called a “duplicate packet problem” when the POSIP is in the administrative down state and connected to a protected circuit. There is no workaround.

- CSCdj86822

Changing the MTU size on a PA-2CE1 port adapter has no effect until the system is reloaded.

IP Routing Protocols

- CSCdj68388

Refer to CSCdk03050 for Release 11.1 integration information. Enhanced IGRP topology entries from the redistribution of connected routes where Enhanced IGRP is already using natively might not clear when the interface goes down.

- CSCdj83029

The router might reload after the **no area area-id** command is used. There is no workaround.

ISO CLNS

- CSCdj73031

DECnet discard routes cause the cached cluster alias and real entries to be transmitted out of the wrong interface.

Wide-Area Networking

- CSCdj71467

Only Cisco 7200 routers are affected by this caveat, which might be exhibited as follows: the router might reload unexpectedly; existing calls are terminated prematurely or are not terminated when expected (based on the settings of the dialer idle timer); the time-to-disconnect listed on calls appears to be wrong.

Cisco 7200 routers that employ optimum/flow switching on dialer interfaces are subject to these symptoms; however, the likelihood of these conditions occurring is rare.

Workaround: Do not enable optimum/flow switching on dialer interfaces when using Release 11.3 images prior to 11.3(1.2). Upgrade to a newer image when available.

Related Documentation

The following sections describe the documentation available for Cisco 7000 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration 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 the documents listed in the following sections:

- Release-Specific Documents, page 28
- Platform-Specific Documents, page 29
- Feature Modules, page 29
- Cisco IOS Software Documentation Set, page 29

Release-Specific Documents

The following documents are specific to Release 11.3. They are located on CCO and the Documentation CD-ROM.

- *Release Notes for Cisco IOS Release 11.3*

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents

To reach these documents from CCO, click on this path:

Service & Support: Technical Documents

- Caveats document

As a supplement to the caveats listed in the “Caveats” section in these release notes, see the *Caveats for Cisco IOS Release 11.3 T* document, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 AA.

To reach the caveats document from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

To reach the caveats document on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

Hardware documentation for the Cisco 7200 family is available on CCO and the Documentation CD-ROM. These documents ship with the Cisco 7200 family.

To access hardware documents on CCO, follow this path:

Service and Support: Documentation Home Page: Cisco Documentation: Core/High-End Routers

To access hardware documentation on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Core/High-End Routers

Feature Modules

Feature modules describe new features supported by Release 11.3 AA and are an update to the Cisco IOS documentation set. Feature modules consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. The feature module information is included in the next printing of the Cisco IOS documentation set.

To reach the feature modules from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

To reach the feature modules on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Cisco IOS Release 11.3

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. These documents are 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 two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, 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 CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

To reach these documents from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Release 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

To reach these documents on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Release 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

Release 11.3 Documentation Set

Table 4 describes the contents of the Cisco IOS Release 11.3 software documentation set. The document set is available in electronic form and also in printed form upon request.

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

To reach the Cisco IOS documentation set from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3

To reach the Cisco IOS documentation set on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Table 4 Cisco IOS Software Release 11.3 Documentation Set

| Books | Chapter Topics |
|---|---|
| <ul style="list-style-type: none">• Configuration Fundamentals Configuration Guide• Configuration Fundamentals Command Reference | Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management |
| <ul style="list-style-type: none">• Network Protocols Configuration Guide, Part 1• Network Protocols Command Reference, Part 1 | IP Addressing IP Services 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> | AppleTalk Novell IPX |
| <ul style="list-style-type: none">• <i>Network Protocols Configuration Guide, Part 3</i>• <i>Network Protocols Command Reference, Part 3</i> | Apollo Domain Banyan VINES DECnet ISO CLNS XNS |
| <ul style="list-style-type: none">• <i>Wide-Area Networking Configuration Guide</i>• <i>Wide-Area Networking Command Reference</i> | ATM Frame Relay SMDS X.25 and LAPB |

Table 4 Cisco IOS Software Release 11.3 Documentation Set (continued)

| Books | Chapter Topics |
|--|--|
| <ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> | AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options |
| <ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Configuration Guide</i> | Interface Configurations |
| <ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> | Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples |
| <ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> | Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing |
| <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 Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies |
| <ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> | Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features |
| <ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> | Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols |
| <ul style="list-style-type: none"> • <i>Configuration Guide Master Index</i> • <i>Command Reference Master Index</i> | |

Table 4 Cisco IOS Software Release 11.3 Documentation Set (continued)

| Books | Chapter Topics |
|---|----------------|
| <ul style="list-style-type: none">• <i>Cisco IOS Software Command Summary</i>• <i>Cisco IOS System Error Messages</i>• <i>Debug Command Reference</i>• <i>Dial Solutions Quick Configuration Guide</i> | |

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs that are described in the “Service and Support” section of the *Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

If you have a CCO login account, you can access the following URL, which contains links and helpful tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Collections of the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—Popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.

- Internetworking Features—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Appliances and Software, Network Management, Network Protection Software and Tips, and WAN Switching Products and Software.
- Special Collections—Other Helpful Documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 28.

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.