



Text Part Number: 78-6989-01 Rev. -B0

# Release Notes for Cisco AS5800 Universal Access Servers/Voice Gateway for Cisco IOS Release 12.0 XL

---

**August 23, 1999**

These release notes for Cisco AS5800 universal access servers/Voice Gateway support Cisco IOS Release 12.0 XL, up to and including Release 12.0(4)XL1. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(4)XL1, see the “Caveats” section on page 19 and *Caveats for Cisco IOS Release 12.0 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

## Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 4
- New and Changed Information, page 12
- Important Notes, page 13
- Caveats, page 19
- Related Documentation, page 20
- Service and Support, page 25
- Cisco Connection Online, page 26
- Documentation CD-ROM, page 27

---

### Corporate Headquarters

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

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

## Introduction

This section contains information about the Cisco AS5800 universal access servers/Voice Gateway and Early Deployment (ED) releases for the Cisco AS5800.

### Cisco AS5800 Universal Access Server

The Cisco AS5800 is a high-density, Integrated Services Digital Network (ISDN) and modem Wide Area Network (WAN) aggregation system that provides digital and analog call termination. It is intended to be used as a service provider dial point-of-presence (POP) or centralized enterprise dial gateway. The Cisco AS5800 consists of a dial shelf, a router shelf, and (optionally) a system controller:

- The Cisco 5814 dial shelf has 14 slots and can support 1 dial shelf controller card and up to 12 feature cards (subject to a limit of 2 trunk cards and 10 modem cards) to provide full analog modem and ISDN coverage. The dial shelf supports up to 720 simultaneous analog and/or digital calls. Analog calls are terminated by a feature card that is loaded with integrated modems. ISDN calls are terminated onboard the trunk card on High-Level Data Link Control (HDLC) controllers. The E1 trunk and the T1 trunk card include channel service units (CSUs) and has either 12 E ports or 12 T1 ports that can operate as Primary Rate Interface (PRI) interfaces or channelized interfaces in any combination.
- The Cisco 7206 router shelf contains a network processing engine, an I/O controller, and the egress interfaces, such as High-Speed Serial Interface (HSSI), Fast Ethernet (FE), Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM), and supports either 280W AC-input or 280W DC-input redundant power. The router shelf also contains a dial shelf interconnect port adapter with a single RJ-45 receptacle that is used to connect the router shelf to the Cisco 5814 dial shelf. The interconnect port adapter connects directly to the dial shelf controller card on the dial shelf via a single, full-duplex cable. The cable used for this connection is a Cisco-proprietary cable, customized with jack screws to secure the connection. You must use this specially designed cable that ships with your interconnect port adapter.
- The Cisco 3640 system controller includes the Cisco 3640 router running Cisco IOS software. The system controller can be installed at a remote facility so users can access multiple systems through a console port or Web interface. System administrators can download software configurations to any Cisco AS5800 universal access server using Simple Network Management Protocol (SNMP) or Telnet. The system controller monitors Cisco equipment to provide performance data collection, accounting data collection, and logging.

The Cisco 5814 dial shelf and host Cisco 7206 router shelf communicate over a dial shelf interconnect cable (DSIC). This nonblocking interconnect supports 100 Mbps, full-duplex data transfer. Data is converted into packets by the feature cards, transmitted to a hub on the dial shelf controller (DSC) card, and from there sent to the router shelf. Conversely, packets from the router shelf are sent to the DSC card, where they are transmitted over the backplane to the modem and trunk cards.

The AC-input power shelf is an optional component of the Cisco AS5800 universal access servers/Voice Gateway and is used to convert AC-input power into DC-output power for the DC-powered Cisco 5814 dial shelf. The AC-input power shelf contains two AC-input power supplies.

The Cisco AS5800 universal access servers/Voice Gateway accept AC-input power via a separate, self-contained AC-input power shelf, which converts AC-input power into DC-output for use by the DC-powered dial shelf. The AC-input power shelf is rack-mounted and has a safety cover that shields the electrical connections in the power shelf rear.

The AC-input to DC-output connection supplies -48V DC-output power to the dial shelf power entry modules (PEMs). The PEMs receive the -48 volts and transmit power to the filter module. Power flows through the filter module to the backplane where it is distributed to the dial shelf controller card(s) and feature cards.

The AC-input power shelf includes two 2,000-watt, AC-input power supplies that plug into a common power backplane in the AC-input power shelf. A single AC-input power supply is capable of powering a fully configured Cisco 5814 dial shelf. The second power supply provides full redundancy.

For more information on the Cisco AS5800, refer to the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide* (DOC-5800-SICG) or the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide* (DOC-5800-HICG) that shipped with your system. You can also access these documents on the Web. See the “Documentation CD-ROM” section on page 27 of these release notes.

## Cisco AS5800/Voice Gateway

The Cisco AS5800/Voice Gateway enables highly scalable deployment of toll-quality voice and fax services over data networks. Enhanced with Cisco's IOS software and Service Node (SN) capabilities, the AS5800 supports features such as pre-paid and post-paid calling card, 800 call redirect, voice activated dialing, and voice and fax mail.

The AS5800 is specifically designed to meet the demands of large service providers such as Post, Telephone, and Telegraphs (PTTs), regional bell operating companies (RBOCs), inter-exchange carriers (IXCs), and large Internet telephony service providers (ITSPs). The physical architecture of the AS5800 product enhances reliability, availability, and serviceability. Critical features to dial POP administrators include minimizing downtime, service costs, and time to deployment. The AS5800 includes hot-swap capability on all cards, load-sharing and redundant hot-swappable power supplies, and redundant shelf controllers. The AS5800 complies with Network Equipment-Building System (NEBS) Level 3 requirements, as defined by Bellcore SR-3580 and European requirements by European Telecommunication Standards Institute (ETSI).

The AS5800 supports up to 1344 voice ports in a single system, thus offering the highest concentration of VoIP Digital Signal Processors (DSPs) available in a single voice gateway. The AS5800 offers breakthrough voice quality, density, and scalability, while continuing to provide the rich set of access, VoIP, and QoS services that are part of Cisco IOS software.

### AS5800 Voice Feature Card

Cisco AS5800 Voice Feature card, is a full featured voice processing card that supports up to 192 DSP-based voice ports. Voice processing capabilities include Voice Activity Detection (VAD), comfort noise generation, adaptive jitter buffering, programmable 16 and 32msec echo cancellation, programmable frame size, and DTMF (Dual Tone Multiple Frequency) detection and generation. The AS5800 Voice Feature card offers industry-leading DSP density and a wide range of VoIP codecs, including G.711, G.729, G.729a, G.723.1, and Group III real-time fax support, on any port at any time.

For information on new features and Cisco IOS commands supported by Release 12.0 XL, see the “New and Changed Information” section on page 12 and “Related Documentation” section on page 20.

## Early Deployment Releases

These release notes describe only Release 12.0 XL for Cisco AS5800 universal access servers/Voice Gateway and do not describe features that are available in Release 12.0 or other Release 12.0 Early Deployment (ED) releases. Release 12.0 XL is an ED release based on Release 12.0 and announces fixes to software caveats and support for new Cisco hardware.

For information about features in Release 12.0, see *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

For information about features in other ED releases, see Table 1.

For information about features in other platforms, see *Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

**Table 1 Early Deployment Releases for the Cisco AS5800 Universal Access Server**

ED Release	Maintenance Release	Additional Software Features	Additional Hardware Features	Availability
Release 12.0 XJ	(4)	None	None	Now
Release 12.0 T	(5)	<ul style="list-style-type: none"> <li>• Cisco IOS Support for IP Connection to SS7 Signalling Controller</li> <li>• Dial Shelf Controller Redundancy</li> </ul>	None	July 1999
Release 11.3 AA	(9)	<ul style="list-style-type: none"> <li>• VPDN Per User Configuration</li> </ul>	None	Now

## System Requirements

This section describes the system requirements for Release 12.0(4)XL1:

- Memory Requirements, page 5
- Hardware Supported, page 5
- Determining the Version of Your Software Release, page 6
- Upgrading to a New Software Release, page 6
- Modem Code Software, page 6
- Feature Set Tables, page 7

## Memory Requirements

Table 2 describes the memory requirements for the Cisco AS5800 platform feature sets supported by Cisco IOS Release 12.0 XL.

**Table 2** Memory Requirements for the Cisco AS5800 Universal Access Server

System Components	Feature Set	Image Name	Software Image	Minimum Flash Memory	Minimum DRAM Memory	Runs From
Cisco AS5800	IP Standard	IP Plus	c5800-p4-mz	16 MB	<ul style="list-style-type: none"> <li>• 128 MB for NPE-200</li> <li>• 256 MB for NPE-300</li> </ul>	RAM
Dial Shelf: Cisco 5814		IP Plus	dsc-c5800-mz	8 MB	32 MB	RAM
Cisco AS5800	Service Provider Standard	Service Provider IPsec 56	c5800-p456i-mz	16 MB	<ul style="list-style-type: none"> <li>• 128 MB for NPE-200</li> <li>• 256 MB for NPE-300</li> </ul>	RAM

## Hardware Supported

Cisco IOS Release 12.0 XL supports the Cisco AS5800 universal access servers/Voice Gateway.

### Platforms

- Cisco AS5814
- Cisco RS7206
- Cisco RS7206 VXR

### Interfaces

- 12 port T 1 or E1 termination card
- Channelized T 3 (CT3) termination card

### Modem Cards

144-modem MICA card

### Voice Feature Card(VFC)

Supports up to 192 DSP-based voice ports

### Optional AC-input Power Shelf

Two AC-input power supplies

### NPE Support

With *any* AS5800 software image, the maximum hardware configuration with an NPE-200 router shelf (RS7206) is one CT3 or two T 1/E 1 trunk cards and five DMMs or 10 HMMs for a maximum of 28 T 1/24 E 1 controllers and 720 modems.

If a larger configuration is desired, a second NPE-200 router shelf can be configured in split-shelf mode, or a single NPE-300 (RS7206 VXR).

The NPE call limitations for an AS5800/Voice Gateway are:

- 672 calls per NPE-200
- 1344 calls per NPE-300

## Determining the Version of Your Software Release

To determine the version of Cisco IOS software running on your Cisco AS5800, log in to the Cisco AS5800 and enter the **show version** EXEC command:

```
5800>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5800 Software c5800-p4-mz, Version 12.0(4)XL1, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

## Modem Code Software

Modem code is either stored in Flash memory or bundled in the Cisco IOS software image. Bundling eliminates the need to store separate modem code images. When the Cisco AS5800 is powered on, the system software unpacks the modem code and loads the proper code on the modem cards.

The **show modemcap** command lists all versions of modem code running on the modem modules, residing in system Flash, and bundled with Cisco IOS software. Enter the **show modemcap** command to help you decide if you need to update your modem code files.

---

**Note** You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

---

The modem code release notes are on CCO and the Documentation CD-ROM:

You can reach the release notes on CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Access Servers and Access Routers: Firmware and Portware Information**

You can reach the release notes on the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Firmware and Portware Information**

## 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.

Release 12.0(4)XL1 supports the same feature sets as Release 12.0(2)T, but Release 12.0(4)XL1 can include new features supported by the Cisco AS5800 universal access servers/Voice Gateway. See Table 3.

**Table 3 Feature Sets Supported by Cisco AS5800 Series Universal Access Servers**

Feature Set	Software Image	Feature Set Matrix Term	Image Name
IP Standard Feature Set	c5800-p4-mz	Basic <sup>1</sup>	IP Plus
	dsc-c5800-mz	Basic	IP Plus
Service Provider Standard Feature Set	c5800-p456i-mz	Basic, IPsec 56 <sup>2</sup>	Service Provider IPsec
	dsc-c5800-mz	Basic	IP Plus

<sup>1</sup> This feature is offered in the Basic feature set.

<sup>2</sup> This feature is offered in the encryption feature sets that consist of 56-bit (IPsec 56) data encryption feature sets.



**Caution** Cisco IOS images with strong encryption (including, but not limited to 168-bit (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 due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 4 lists the features and feature sets supported by the Cisco AS5800 universal access servers/Voice Gateway in Cisco IOS Release 12.0 XL and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (4) means a feature was introduced in 12.0(4)XL1. If a cell in this column is empty, the feature was included in the initial base release.

---

**Note** This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

---

**Table 4 Feature List by Feature Set for the Cisco AS5800 Series Universal Access Servers**

Features	Software Images by Feature Set		
	In	IP Plus	Service Provider IPsec 56
<b>IBM Support</b>			
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		No	No
Cisco MultiPath Channel (CMPC)		No	No
DLSw+ Enhancements		No	No
FRAS Enhancements		No	No
RIF Passthru in DLSw+		No	No
SRB over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers		No	No
TN3270 LU Nailing		No	No
TN3270 Server Enhancements		No	No
Token Ring LANE		No	No
Tunneling of Asynchronous Security Protocols		No	No
<b>Internet</b>			
DRP Server Agent		No	No
DRP Server Agent Enhancements		No	No
L2TP	(1)	Yes	No
Signaling System 7 (SS7)		Yes	Yes
<b>IP Routing</b>			
Easy IP (Phase 1)		Yes	Yes
Easy IP (Phase 2)	(1)	Yes	No
DHCP Server			
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations		No	No
IP Enhanced IGRP Route Authentication	(1)	Yes	Yes
OSPF LSA Group Pacing	(1)	Yes	Yes
OSPF Point-to-Multipoint Networks with Neighbors	(1)	Yes	Yes
Per User DNS		No	No
PIM Version 2	(1)	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco AS5800 Series Universal Access Servers (continued)**

Features	Software Images by Feature Set		
	In	IP Plus	Service Provider IPsec 56
TCP Enhancements: — TCP Selective Acknowledgment — TCP Timestamp	(1)	Yes	Yes
<b>LAN Support</b>			
AppleTalk Access List Enhancements		No	No
DECnet Accounting		No	No
IPX Named Access Lists		No	No
IPX SAP-after-RIP		No	No
NLSP Enhancements		No	No
NLSP Multicast Support		No	No
<b>Management</b>			
Cisco Call History MIB Command Line Interface	(1)	Yes	Yes
Cisco IOS File System	(1)	Yes	No
Cisco IOS Internationalization	(1)	Yes	Yes
Conditionally Triggered Debugging	(1)	Yes	Yes
Entity MIB, Phase 1	(1)	Yes	Yes
External Portware Download		No	No
Show Caller Command		No	No
Show Modem Command		No	No
SNMP v2C	(1)	Yes	Yes
SNMP v3	(3)	Yes	No
SNMP Inform Requests		No	No
Virtual Profiles	(1)	Yes	Yes
VPDN MIB	(1)	No	No
VPDN MIB and Syslog Facility		No	No
<b>Multimedia</b>			
IP Multicast Load Splitting across Equal-Cost Paths	(1)	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	(1)	Yes	Yes
IP Multicast over Token Ring LANs	(1)	Yes	Yes
Stub IP Multicast Routing	(1)	Yes	Yes
<b>Quality of Service</b>			
CLI String Search	(1)	Yes	No
RTP Header Compression		No	No
<b>Security</b>			

## System Requirements

**Table 4 Feature List by Feature Set for the Cisco AS5800 Series Universal Access Servers (continued)**

Features	Software Images by Feature Set		
	In	IP Plus	Service Provider IPsec 56
AAA Scalability		No	No
Authenticating ACL		No	No
Automated Double Authentication		No	No
Certificate Authority Interoperability		No	No
Double Authentication	(1)	Yes	Yes
Encrypted Kerberized Telnet		No	No
HTTP Security	(1)	Yes	Yes
Internet Key Exchange Security Protocol		No	No
IPsec Network Security		No	No
MS-CHAP Support		No	No
Named Method Lists for AAA Authentication and Accounting		No	No
Per-User Configuration	(1)	Yes	Yes
Reflexive Access Lists	(1)	Yes	Yes
TCP Intercept		No	No
Vendor-Proprietary RADIUS Attributes	(1)	Yes	Yes
Vendor-Proprietary RADIUS-Additional Attributes		No	No
<b>Switching</b>			
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No	No
CLNS and DECnet Fast Switching over PPP		No	No
DECnet/Vines/XNS over ISL		No	No
Fast-Switched Policy Routing	(1)	Yes	Yes
IPX Routing over ISL Virtual LANs		No	No
VIP Distributed Switching Support for IP Encapsulated in ISL		No	No
<b>Terminal Services</b>			
Telnet Extensions for Dialout		No	No
Virtual Templates for Protocol Translation		No	No
<b>WAN Optimization</b>			
ATM MIB Enhancements		No	No
PAD Enhancements		No	No
PAD Subaddressing	(1)	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco AS5800 Series Universal Access Servers (continued)**

Features	Software Images by Feature Set		
	In	IP Plus	Service Provider IPSec 56
<b>WAN Services</b>			
Always On/Dynamic ISDN (AO/DI)		No	No
Bandwidth Allocation Control Protocol	(1)	Yes	Yes
Channelized T3		No	No
Dialer Watch	(1)	Yes	Yes
Dynamic Multiple Encapsulation for Dial-in over ISDN	(4)T	Yes	Yes
E1 R2	(3)	Yes	Yes
E1 R1 Support for Taiwan only	(3)	Yes	Yes
Enhanced Local Management Interface (ELMI)		No	No
Frame Relay Enhancements	(1)	Yes	Yes
Frame Relay MIB Extensions	(1)	Yes	Yes
Frame Relay Router ForeSight	(1)	Yes	Yes
GRE VPN		No	No
ISDN Advice of Charge	(1)	Yes	Yes
ISDN Caller ID Callback	(1)	Yes	Yes
ISDN NFAS	(1)	Yes	Yes
Layer 2 Forwarding—Fast Switching	(1)	Yes	Yes
Leased-Line ISDN at 128 kbps		No	No
Microsoft Point-to-Point Compression (MPPC)		No	No
MS Callback	(1)	Yes	Yes
Modem Management Enhancements	(1)	Yes	Yes
Multiple ISDN Switch Types		No	No
National ISDN Switch Types for BRI and PRI Interfaces (NI2)		No	No
PPP over ATM		No	No
Stackable Home Gateway		No	No
Switched 56K Digital Connections		No	No
Telnet Extensions for Dialout		No	No
X.25 Enhancements	(1)	Yes	Yes
X.25 on ISDN	(1)	Yes	Yes
<b>Miscellaneous</b>			
Async over UDP	(3)	Yes	No
CNS Client for Cisco IOS Software	(5)	No	Yes

**Table 4 Feature List by Feature Set for the Cisco AS5800 Series Universal Access Servers (continued)**

Features	Software Images by Feature Set		
	In	IP Plus	Service Provider IPsec 56
CT3 Channelized T3 Trunk Card	(3)	No	No
CT3 Redundancy, Phase I	(3)	Yes	Yes
Flashpoint	(5)	Yes	Yes
Generic System File Layer (OS_IFSS)	(1)	Yes	No
L2TP Dial-Out	(5)	Yes	Yes
L2TP Support for VPDN	(5)	Yes	No
Parse Bookmarks	(1)	Yes	No
Policy Routing Infrastructure Update	(3)	Yes	No
Process MIB	(3)	Yes	No
Resource Pool Management	(5)	No	No
Cisco IOS Support for IP Connection to SS7 Signalling Controller	(3)	Yes	Yes
Voice over IP	(4)XL	Yes	Yes

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5800 universal access servers/Voice Gateway for Release 12.0 XL.

### New Features in Release 12.0(4)XL1

#### Voice over IP on the Cisco AS5800

Voice over IP (VoIP) enables a Cisco AS5800 universal access server to provide enhanced voice and fax traffic, such as telephone calls and faxes, over an IP network. Voice over IP is primarily a software feature; however, to use this feature on the Cisco AS5800, you must install a VoIP feature card (VFC). The VFC uses the Cisco AS5800's T1/E1 and T3 Public Switched Telephone Network (PSTN) interfaces and local area network (LAN) or wide area network (WAN) routing capabilities to provide up to a 192 ports or channels (per VFC card) for VoIP packetized voice traffic.

VoIP on the Cisco AS5800 has the following primary applications:

- Two-Stage-Dial Toll Bypass
- PSTN Voice-Traffic and Fax-Traffic Offload
- Universally Accessible Voice-Mail and Fax-Mail Services

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco AS5800 universal access servers/Voice Gateway.

### Cisco IOS Syslog Failure

Certain versions of Cisco IOS software can fail 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 that cause these 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 needs to be reconfigured by its administrator. Some Cisco IOS devices can hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must visit the 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 indicate that they were “restarted by power-on,” even when that was not the case.

Assume that any potential attacker knows the existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

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

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

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

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

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

### Affected Devices and Software Versions

Table 5 describes hardware and software that are affected by this problem. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 5. Cisco is correcting the problem in certain special releases, will correct it in future maintenance and interim releases, and intends to provide fixes for all affected IOS variants. See Table 5, *Affected and Repaired Software Versions* for details.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” section on page 15 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 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 enter the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System Software.” Other Cisco devices do not have the **show version** command and 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 problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- 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
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug 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 5 gives Cisco’s projected fix dates.

Make sure that your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release, for example, from 11.2[11]P to 11.2[17]P, but it is often a factor when you upgrade between major releases, for example, from 11.2 P to 11.3 T.

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require you to upgrade to a new major release. Cisco recommends that you carefully plan 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>

If you have service contracts, you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to only obtain the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. You can only upgrade to the software described in one row of Table 5—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](mailto:tac@cisco.com)

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Customers with no contracts must request for free updates through the TAC. For software updates, please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)."

## Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to port 514. You can do this by 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, apply it to all interfaces to which attackers can send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces—as well as virtual interfaces and 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.

No single input access list works in all configurations. Be sure you 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 problem:

```
! 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 can 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—and traffic destined to the device. If the IOS device is expected to forward syslog packets, you will have to filter in detail. 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 Cisco IOS Release 12.0(2) is vulnerable, as are interim Releases 12.0(2.1) to 12.0(2.3). The first fixed interim version of Release 12.0 mainline software is Release 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 Release 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 Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 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 Release 12.0(2a) is to Release 12.0(3).

---

**Note** All dates within this table are subject to change.

---

Table 5 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix <sup>1</sup>	First Fixed Interim Release <sup>2</sup>	Fixed Maintenance Release <sup>3</sup>
<b>Unaffected Releases</b>				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
<b>Releases Based on 11.3</b>				
11.3 AA	11.3 early deployment for Cisco AS5800	11.3(7)AA2, 15-FEB-1999 <sup>4</sup>	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 15-FEB-1999
<b>Releases Based on 12.0</b>				
12.0	12.0 Mainline	12.0(2a), 15-FEB-1999	12.0(2.4)	12.0(3), 15-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 15-FEB-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 15-FEB-1999	12.0(2)S <sup>5</sup> , 15-FEB-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 15-FEB-1999
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-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 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 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T 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 12.0 T at 12.0(3)T	12.0(2)XC1, 15-FEB-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 15-FEB-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 15-FEB-1999	Merged	Upgrade to 12.0(3)T

## Important Notes

---

- 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 can 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 and are 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.

## Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-\* MIBs are currently migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 6:

**Table 6**            **Deprecated and Replacement MIBs**

<b>Deprecated MIB</b>	<b>Replacement</b>
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
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	
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	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

## Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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

All caveats in Release 12.0 and Release 12.0 T are also in Release 12.0 XL.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*.

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*, which lists severity 1 and 2 caveats, and 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. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at <http://www.cisco.com/support/bugtools>.

---

## Open Caveats—Release 12.0(4)XL1

This section describes possibly unexpected behavior by Release 12.0(4)XL1.

### Miscellaneous

- CSCdm36607  
L2TP tunnels between Cisco AS5300s and the Cisco 7200 series router are dropping several times every hour.
- CSCdm44249  
Reusing the same CE address on two CEs connected to the same PE, in different VRFs, does not work properly in the case where the link between the PE and CE is ethernet.
- CSCdm49454  
When **cable ip-broadcast-echo** is enabled, under certain timing conditions may cause a buffer leak. The workaround is do not enable **cable ip-broadcast-echo** and **cable ip-multicast-echo**.

### Wide-Area Networking

- CSCdm34846  
The router reloads when the **ip rtp header-compression** command is unconfigured and encapsulation is changed from PPP to Frame Relay.
- CSCdm45278  
Incoming ISDN BRI calls may crash at `process_dialer_command()` when Channel ID 0x88 is received in the incoming SETUP messages.
- CSCdm48075  
By default, LANE FSSRP is now completely off on all subinterfaces and all LANE components.  
To turn this feature on, use the interface config command: **lane fssrp**  
When entered, this command recycles all LANE components on that interface and its subinterfaces.

## Resolved Caveats—Release 12.0(4)XL1

Because Release 12.0(4)XL1 is the initial base release, there are no resolved caveats.

## Related Documentation

The following sections describe the documentation available for the Cisco AS5800 universal access servers/Voice Gateway. 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 these documents:

- Release-Specific Documents, page 20
- Platform-Specific Documents, page 21
- Feature Modules, page 21
- Cisco IOS Software Documentation Set, page 22

## Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

On CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes**

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

**Service & Support: Technical Documents**

- *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*

As a supplement to the caveats listed in “Caveats” in these release notes, see *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0 XL.

On CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats**

---

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

---

## Platform-Specific Documents

These documents are available for the Cisco AS5800 universal access servers/Voice Gateway on CCO and the Documentation CD-ROM:

**Table 7 Cisco AS5800 Universal Access Server—Related Documents**

Cisco Product	Document Title
Cisco AS5800 universal access server	<ul style="list-style-type: none"> <li>• <i>Cisco AS5800 Universal Access Server Hardware Installation and Configuration Guide</i></li> <li>• <i>Cisco AS5800 Universal Access Server Regulatory Compliance and Safety Information</i></li> <li>• <i>Cisco AS5800 Universal Access Server Software Installation and Configuration Guide</i></li> <li>• Configuration notes, updates, feature modules, and release notes</li> </ul>
Cisco 7206 router shelf	<ul style="list-style-type: none"> <li>• <i>Cisco 7206 Installation and Configuration Guide</i></li> <li>• <i>Regulatory Compliance and Safety Information for the Cisco 7206</i></li> <li>• Configuration notes, updates, feature modules, and release notes</li> </ul>
Cisco 3640 system controller	<ul style="list-style-type: none"> <li>• <i>Cisco 3640 Router Installation and Configuration Guide</i></li> <li>• <i>Cisco 3640 System Controller Installation and Configuration Guide</i></li> <li>• <i>Regulatory Compliance and Safety Information for the Cisco 3640</i></li> <li>• Configuration notes, updates, feature modules, and release notes</li> </ul>
Cisco IOS software	<ul style="list-style-type: none"> <li>• Configuration guides</li> <li>• Command references</li> <li>• Feature modules, configuration notes, updates, and release notes</li> </ul>

On CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800**

## Feature Modules

Feature modules describe new features supported by Release 12.0 XL and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation**

## 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, which 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.

You can reach these documents on CCO at:

**Service & Support: Technical Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

You can reach these documents on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

### Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and 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 hard-copy documents were printed.

---

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

**Service & Support: Technical Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

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

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

**Table 8 Cisco IOS Software Release 12.0 Documentation Set**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging 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 Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	AppleTalk Novell IPX

**Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
<ul style="list-style-type: none"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

---

**Note** *Cisco Management Information Base (MIB) User Quick Reference* 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, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco 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 Technical Assistance Center Home Page

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

[http://www.cisco.com/kobayashi/serv\\_tips.shtml](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—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes 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—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.

- Special Collections—Lists 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](http://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](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto: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](mailto: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](mailto: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 20.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratum, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R)

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

