



Text Part Number: 78-6916-02

Release Notes for Cisco AS5200 Series Universal Access Servers for Cisco IOS Release 12.0 XI

June 17, 1999

These release notes for Cisco AS5200 series universal access servers support Cisco IOS Release 12.0 XI, up to and including Release 12.0(4)XI. 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)XI, see the “Caveats” section on page 14 and *Caveats for Cisco IOS Release 12.0T*. 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* on CCO and the Documentation CD-ROM.

Contents

These release notes cover the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 8
- Important Notes, page 8
- Caveats, page 14
- Related Documentation, page 14
- Service and Support, page 19
- Cisco Connection Online, page 20
- Documentation CD-ROM, page 21

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 AS5200 series universal access servers and Early Deployment (ED) Releases for the Cisco AS5200.

Cisco AS5200

The Cisco AS5200 universal access server is a multifaceted data communications platform that provides all the functions of an access server, a router, modems, and terminal adapters (TAs) in a modular chassis. Mid-sized organizations or service providers requiring centralized processing capabilities for mobile users and telecommuters will benefit the most using the Cisco AS5200 universal access server.

With their optimization for high-speed modem access, the Cisco AS5200 universal access servers are ideally suited for all traditional dial-up applications, such as host access, electronic mail, file transfer, and dial-in access to a local area network.

For information on new features and Cisco IOS commands supported by Release 12.0(4)XI, see the “New and Changed Information” section on page 8 and “Related Documentation” section on page 14.

Early Deployment Releases

These release notes describe only Release 12.0 XI for Cisco AS5200 series universal access servers and do not describe features that are available in Release 12.0 or other Release 12.0 Early Deployment (ED) releases. Release 12.0(4)XI is an Early Deployment (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 platforms, see *Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

System Requirements

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

- Memory Requirements, page 3
- Hardware Supported, page 3
- Determining the Version of Your Software Release, page 4
- Upgrading to a New Software Release, page 4
- Modem Code, page 4
- Feature Set Tables, page 5

Memory Requirements

Table 1 describes the memory requirements of the Cisco IOS feature sets for the Cisco AS5200 series universal access servers for Release 12.0(4)XI.

Table 1 Memory Requirements for Cisco AS5200 Series

Feature Sets	Image Name	Software Image	Flash Memory Required	DRAM Memory Required	Runs from
IP Standard Feature Set	IP	c5200-i-1	16 MB	8 MB	Flash
	IP Plus	c5200-is-1	16 MB	8 MB	Flash
	IP Plus (Dual Bank)	c5200-i4s-1	16 MB	8 MB	RAM
IP/IPX/AT/DEC Standard Feature Set	IP/IPX/AT/DEC	c5200-d-1	16 MB	8 MB	Flash
	IP/IPX/AT/DEC Plus	c5200-ds-1	16 MB	8 MB	Flash

Hardware Supported

Cisco IOS Release 12.0 XI supports the Cisco AS5200 series universal access servers.

The following are LAN interfaces supported on the Cisco AS5200:

- Ethernet (AUI)
- MultiChannel Interface (Channelized E1/T1)

The following are WAN data rates supported on the Cisco AS5200:

- 48/56/64 kbps
- 1.544/2.048 Mbps

The following are WAN interfaces supported on the Cisco AS5200:

- EIA/TIA-232
- X.21
- V.35
- EIA/TIA-449
- EIA-530
- ISDN PRI
- E1-G.703/G.704
- Channelized T1
- Channelized E1
- Serial

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 8.

Determining the Version of Your Software Release

To determine the version of Cisco IOS software running on your Cisco AS5200, log in to the Cisco AS5200 and enter the **show version** EXEC command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5200 Software (c5200-i-1), Version 12.0(4)XI, 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

Cisco IOS Release 11.2(2) and later releases, including Release 12.0(4)T, include bundled modem code for the Cisco AS5200, which is the firmware or portware that runs on the Microcom 12-port and MICA 6-port modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the Cisco AS5200 access server starts, the Cisco IOS software unpacks the modem code and loads the proper code on the modem cards. Table 2 lists the current bundled modem code versions for the Cisco AS5200.

Table 2 Current Bundled Modem Code Version

Modem Code Module	Current Bundled Modem Code Version	Cisco IOS Software Releases
Microcom modems	Microcom version 3.3.20	Release 11.3(5)T and later
MICA modems	MICA portware Version 2.3.1.0	Release 11.3(5)T and later

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: Documentation Home Page: 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)XI supports the same feature sets as Release 12.0(4)T, but Release 12.0(4)XI can include new features supported by the Cisco AS5200 series universal access servers.

Table 3 Feature Sets Supported by Cisco AS5200 Series Universal Access Servers

Feature Sets	Image Names	Feature Set Matrix Term	Software Image
IP Standard Feature Set	IP	Basic ¹	c5200-i-1
	IP Plus	Plus ²	c5200-is-1
	IP Plus (Dual Bank)	Plus ³	c5200-14s-1
IP/IPX/AT/DEC Standard Feature Set	IP/IPX/AppleTalk/DEC	Basic	c5200-d-1
	IP/IPX/AppleTalk/DEC Plus	Plus	c5200-ds-1

1 This feature set is offered in the basic feature set.

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

3 This feature set is offered in the Plus feature set.



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

Table 4 lists the features and feature sets supported by the Cisco IOS Release 12.0(4)XI for the Cisco AS5200 series universal access servers. This table uses the following conventions to identify features:

- 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). 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 AS5200 Universal Access Server

Features	In ¹	Software Images by Feature Set				
		IP	IP Plus	IP Plus (Dual Bank)	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
Connectivity						
Layer 2 Tunnel Protocol (L2TP)	(1)T	No	Yes	Yes	No	Yes
IBM Support						
Bridging Code Rework		Yes	Yes	No	Yes	Yes
RIF Passthru in DLSw+		No	No	No	No	No
IP Routing						
Easy IP Phase 2-DHCP Server	(1)T	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes
Per User DNS		Yes	Yes	Yes	Yes	Yes
Management						
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)T	Yes	Yes	Yes	Yes	Yes
Show Caller		Yes	Yes	Yes	Yes	Yes
SNMP Inform Request		No	No	Yes	No	No
SNMP Manager		Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility		No	Yes	Yes	No	Yes
Multimedia						
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	Yes	Yes
Quality of Service						
CLI String Search	(1)T	Yes	Yes	Yes	Yes	Yes
Scalability						
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes	Yes
Security						
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes
Authenticating ACLs		Yes	Yes	Yes	Yes	Yes
Automated Double Authentication		Yes	Yes	Yes	Yes	Yes
MS-CHAP Support		No	No	Yes	No	No
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco AS5200 Universal Access Server (continued)

Features	In ¹	Software Images by Feature Set				
		IP	IP Plus	IP Plus (Dual Bank)	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
Subblock Phase 1		Yes	Yes	Yes	Yes	Yes
WAN Optimization						
DRP Server Agent Enhancement		Yes	Yes	Yes	No	Yes
WAN Services						
Always On/Dynamic ISDN (AO/DI)		No	No	Yes	No	No
ATM E.164 Auto Conversion		Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes
Layer 2 Tunneling Protocol	(1)T	No	Yes	Yes	No	Yes
Microsoft Point-to-Point (MPPC)		Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types		Yes	Yes	Yes	Yes	Yes
Signaling System 7		No	Yes	Yes	No	Yes
Stackable Home Gateway		No	Yes	Yes	No	Yes
Miscellaneous						
Asynch over UDP	(4)T	Yes	Yes	Yes	Yes	Yes
Cisco SNMP Version 3	(4)T	Yes	Yes	Yes	Yes	Yes
CNS Client for Cisco IOS Software	(4)T	No	No	Yes	No	No
Dynamic Multiple Encapsulation for Dial-in over ISDN	(4)T	Yes	Yes	Yes	Yes	Yes
Flow Random Early Detection (Flow WRED)	(4)	Yes	Yes	Yes	Yes	Yes
Generic Filesystem Layer (OS_IFSS)	(4)T	Yes	Yes	Yes	Yes	Yes
ISDN LAPB-TA	(4)T	Yes	Yes	Yes	Yes	Yes
Large Scale Dialout	(4)T	Yes	Yes	Yes	No	No
Multilink Inverse Multiplexor	(4)T	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks	(4)T	Yes	Yes	Yes	Yes	Yes
Process MIB	(4)T	Yes	Yes	Yes	Yes	Yes
Signaling System 7 (SS7)	(4)T	No	Yes	Yes	No	Yes
SLIP-PPP Banner and Banner Tokens	(4)T	No	No	Yes	No	No
Virtual Console	(1)T	Yes	Yes	Yes	Yes	Yes

¹ This column indicates the maintenance release in which the feature was introduced. If this cell is empty in this column, this feature was introduced in the initial base release.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5200 series universal access servers in Cisco IOS Release 12.0(4)XI.

New Software Features in Cisco IOS Release 12.0(4)XI

The following software features are supported by the Cisco AS5200 series universal access servers for Release 12.0(4)XI.

Resource Pool Management

The Resource Pool Manager differentiates wholesale dial customers by using configurable Customer Profiles that are based on the dialed number (DNIS) and Call Type determined at the time of an incoming call or by Domain Name after the call is answered. Each configured Customer Profile will include a maximum allowed session value and an overflow value. As sessions are started and ended in the NAS, session counters for each Customer Profile are incremented and decrements in the NAS. Based upon service-level agreements, customers will be given the appropriate call treatment when the session limit is reached.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that might apply to the Cisco AS5200.

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 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 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
- 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

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 10 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

Important Notes

- 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

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” or “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—as well as 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 version 12.0(2) is vulnerable, as are interim versions 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.

Important Notes

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 ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Unaffected Releases				
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
Releases Based on 11.3				
11.3 AA	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
11.3 DB	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
12.0 T	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
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S ⁵ , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-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.

Table 5 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
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, 7-JAN-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, 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 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

Deprecated MIB	Replacement
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 XI.

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)XI

This section describes possibly unexpected behavior by Release 12.0(4)XI. Unless otherwise noted, these caveats apply to all 12.0 releases up to and including 12.0(4)XI.

Basic System Services

- CSCdk26221

The following cli command does not function : **snmp-server packetsize**. The maximum snmp packetsize for 12.0(3)T is fixed at 484. There is no known workaround.

Miscellaneous

- CSCdk55110

When tunneling IPX over an IP tunnel, and when using an extended inbound access list for ip on the tunnel interface, the ipx traffic gets blocked by the access list. As a workaround a "permit gre" statement could be added in the extended access-list.

Resolved Caveats—Release 12.0(4)XI

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

Related Documentation

The following sections describe the documentation available for the Cisco AS5200 series universal access servers. 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 Documentation, page 15
- Platform-Specific Documents, page 15
- Feature Modules, page 16
- Cisco IOS Software Documentation Set, page 16

Release-Specific Documentation

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: Documentation Home Page: 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 12.0T*

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(4)T.

On CCO at:

Service & Support: Documentation Home Page: 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 AS5200 series universal access servers on CCO and the Documentation CD-ROM.

- *Cisco AS5200 Universal Access Server Installation Guide*
- *Cisco AS5200 Universal Access Server Software Configuration Guide*
- *Cisco AS5200 Manager Guide*

- Modem/Terminal Adapter Information
- *Regulatory Compliance and Safety Information*
- Documentation for Spare Parts
- Release Notes

On CCO at:

Service & Support: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5200

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5200

Feature Modules

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

On CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 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: Documentation Home Page: 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 7 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: Documentation Home Page: 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 7 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<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 Cisco Mainframe Channel Connection Airline Product Set

Table 7 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	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"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Overview IP Addressing and 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> 	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<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 Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB

Table 7 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<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 Frame Relay-ATM Internetworking Synchronized Clocks 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> 	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"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> 	

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

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
- 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 documents mentioned in the "Related Documentation" section on page 14.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, 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, Stratm, 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. (9905R)

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