



Text Part Number: 78-6133-04

Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.0

February 8, 1999

These release notes describe new features and significant software components for the Cisco uBR7200 series universal broadband routers that support Cisco IOS Release 12.0, up to and including Release 12.0(3). These release notes are updated as needed to accommodate new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes.

For a list of the software caveats that apply to Release 12.0, refer to the *Caveats for Cisco IOS Release 12.0* document that accompanies these release notes. The caveats document is updated for every maintenance release, and is location on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the “Caveats” section on page 14 of these release notes.

Use these release notes with the cross-platform *Release Notes for Cisco IOS Release 12.0* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 7
- Important Notes, page 7
- Caveats, page 14
- Related Documentation, page 14
- Service and Support, page 18
- Cisco Connection Online, page 13
- Documentation CD-ROM, page 14

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 on the Cisco uBR7200 series universal broadband routers.

Cisco Data-over-Cable Products

The Cisco data-over-cable products—the Cisco uBR7223 universal broadband router, the Cisco uBR7246 universal broadband router, and the Cisco uBR904 cable modem—are compliant with Multimedia Cable Network Partners, Ltd. (MCNS) specifications. MCNS is a consortium of cable television companies whose goal is to create standards for interoperable data over cable systems.

For more information on the Cisco uBR7200 series universal broadband routers, refer to the “New and Changed Information” section on page 7.

Cisco uBR7223 Universal Broadband Router

The Cisco uBR7223 is a cost-effective, scalable interface between subscriber cable modems and the backbone data network, and is designed specifically for small to medium-sized network installations. The Cisco uBR7223 is based on the Cisco uBR7246.

Cisco uBR7246 Universal Broadband Router

The Cisco uBR7246 is the first of Cisco’s data-over-cable products designed to allow two-way transmission of digital data over hybrid fiber coaxial (HFC) cable. The Cisco uBR7246 supports Internet Protocol (IP) routing with a wide variety of protocols and any combination of Ethernet, Fast Ethernet, High-Speed Serial Interface (HSSI), and Asynchronous Transfer Mode (ATM) media. The Cisco uBR7246 universal broadband router gives cable operators a cost-effective, scalable, and feature-rich interface between subscriber cable modems and the backbone data network.

Cisco uBR904 Cable Modem

The Cisco uBR904 cable modem is the subscriber unit, a key component within a cable data system. This subscriber unit functions as an interface between the subscriber’s personal computer and the cable operator’s network within the subscriber’s small office or home office.

For more information on Cisco uBR904, refer to the “Related Documentation” section on page 14.

System Requirements

This section describes the system requirements for Release 12.0 and includes the following sections:

- Memory Requirements, page 3
- Hardware Supported, page 3
- Determining Your Cisco IOS Software Release, page 4
- Upgrading to a New Release, page 4
- Feature Set Tables, page 5

Memory Requirements

Table 1 describes the memory requirements for the Cisco uBR7200 series for Release 12.0. Cisco uBR7200 series routers are shipped with a 16- or 20-MB Flash memory card.

Table 1 Memory Requirements for the Cisco uBR7200 Series

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From	Feature Status
MCNS Two-Way	ubr7200-p-mz	16 MB Flash	32 MB DRAM	RAM	Added in 12.0(1)

Hardware Supported

Cisco IOS Release 12.0 supports the Cisco uBR7200 series universal broadband routers:

- Cisco uBR7223
- Cisco uBR7246

For detailed descriptions of the new hardware features for Release 12.0, refer to the cross-platform *Release Notes for Cisco IOS Release 12.0*.

Cisco IOS Release 12.0 supports the Cisco uBR7200 universal broadband routers and the MC11 cable modem cards installed in the Cisco uBR7200 series routers. The MC11 cable modem cards provide connection to the hybrid fiber-coaxial network, offering one upstream port and one downstream port. The cable modem card slots are numbered from top to bottom: cable modem card slot 3, slot 4, slot 5, and slot 6.

Table 2 Supported Interfaces on the Cisco uBR7200 Series

Interface, Network Module, or Data Rate	Product Number ¹	Description	Platforms Supported
ATM	PA-A1-OC3SMI	1-port ATM OC-3c/STM-1 single-mode intermediate reach port adapter	Cisco uBR7200 series
	PA-A1-OC3MM	1-port ATM OC-3c/STM-1 multimode port adapter	Cisco uBR7200 series
	PA-A2-4E1XC-OC3SM	5-port ATM CES ² (4 E1 120-ohm CBR ³ ports and 1 OC-3 ATM single-mode port) port adapter	Cisco uBR7246 only
	PA-A2-4E1XC-E3ATM	5-port ATM CES ² (4 E1 120-ohm CBR ³ ports and 1 E3 ATM port) port adapter	Cisco uBR7246 only
	PA-A2-4T1C-OC3SM	5-port ATM CES ² (4 T1 CBR ³ ports and 1 OC-3 ATM single-mode port) port adapter	Cisco uBR7246 only
	PA-A2-4T1C-T3ATM	5-port ATM CES ² (4 T1 CBR ³ ports and 1 T3 ATM port) port adapter	Cisco uBR7246 only
Ethernet	PA-4E	4-port Ethernet 10BaseT port adapter	Cisco uBR7200 series
	PA-8E	8-port Ethernet 10BaseT port adapter	Cisco uBR7200 series
	PA-FE-TX	1-port 100BaseTX Fast Ethernet port adapter	Cisco uBR7200 series
	PA-FE-FX	1-port 100BaseFX Fast Ethernet port adapter	Cisco uBR7200 series
High Speed Serial Interfaces (HSSI)	PA-H	1-port HSSI port adapter	Cisco uBR7200 series

Table 2 Supported Interfaces on the Cisco uBR7200 Series

Interface, Network Module, or Data Rate	Product Number ¹	Description	Platforms Supported
Packet-Over-SONET (POS)	PA-POS-OC3SML	1-port POS OC-3 single-mode, long reach port adapter	Cisco uBR7200 series
	PA-POS-OC3SMI	1-port OC3 single-mode, intermediate reach port adapter	Cisco uBR7200 series
	PA-POS-OC3MM	1-port POS OC3 multimode port adapter	Cisco uBR7200 series
Serial	PA-4T+	4-port synchronous serial port adapter	Cisco uBR7200 series
	PA-8T-232	8-port EIA/TIA-232 synchronous serial port adapter	Cisco uBR7200 series
	PA-8T-V35	8-port V.35 synchronous serial port adapter	Cisco uBR7200 series
	PA-8T-X21	8-port X.21 synchronous serial port adapter	Cisco uBR7200 series
	PA-4E1G-75	4-port unbalanced (75-ohm) E1-G.703/G.704 synchronous serial port adapter	Cisco uBR7200 series
	PA-4E1G-120	4-port balanced (120-ohm) E1-G.703/G.704 synchronous serial port adapter	Cisco uBR7200 series

¹ Refer to CCO or the Documentation CD-ROM for the most current list of supported port adapters.

² CES = circuit emulation services.

³ CBR = constant bit rate.

Determining Your Cisco IOS Software Release

To determine the version of Cisco IOS software currently running on the Cisco uBR7200 series router, log into the router and use the **show version EXEC** command. The following is sample output from the **show version** command. The version number is indicated on the second line as shown below:

```
Cisco Internetwork Operating System Software
IOS (tm) 7246 Software (C7246-JS-L), Version 12.0(3), RELEASE SOFTWARE
```

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

Upgrading to a New Release

For information about upgrading to a new software release, refer to the *Cisco IOS Software Release 12.0 Upgrade Paths and Packaging Simplification* product bulletin located at the following URL: <http://www.cisco.com/kobayashi/library/12.0/120MigrPaths.pdf>

Alternatively, if you do not have an account on CCO, you can access general information about upgrading to a new software release by referring to the *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification (#703: 12/97)* product bulletin located on CCO.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 12.0**, click on **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**. This product bulletin does not contain information specific to Cisco IOS Release 12.0 but provides generic upgrade information that may apply to Cisco IOS Release 12.0

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.

Table 3 lists the Cisco IOS software feature sets available for the Cisco uBR7200 series in Cisco IOS Release 12.0(3).

Table 3 Feature Sets Supported by the Cisco uBR7246

Feature Set	Software Image	Feature Set Matrix Term	Software Image
MCNS Two-Way	MCNS Two-Way	Basic ¹	ubr7200-p-mz

¹ This feature is offered in the basic feature set.

Table 4 lists the features and feature sets supported by the Cisco IOS Release 12.0 for the Cisco uBR7200 series. Table 4 uses the following conventions to identify features:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.

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

Table 4 Feature List by Feature Set for the Cisco uBR7200 Series

Features	MCNS Two-Way Feature Set
Internet	
DRP Server Agent	Yes
IP Routing	
IP Type of Service and Precedence for GRE Tunnels	Yes
Easy IP (Phase 1)	Yes
Hot Standby Router Protocol (HSRP) over ISL and Virtual LAN Configurations	Yes
IP Enhanced IGRP Route Authentication	Yes
OSPF Point to Multipoint	Yes
Management	
Cisco IOS File System	Yes
Entity MIB	Yes
Expression MIB	Yes
Conditionally Triggered Debugging	Yes
SNMP Manager	Yes
Cisco Call History MIB Command Line Interface	Yes
Cisco IOS Internationalization	Yes
SNMPv2C	Yes
Virtual Profiles	Yes

Table 4 Feature List by Feature Set for the Cisco uBR7200 Series (continued)

Features	MCNS Two-Way Feature Set
VPDN MIB and Syslog Facility	Yes
Multimedia	
IP Multicast Load Splitting across Equal-Cost Paths	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	Yes
IP Multicast over Token Ring LANs	Yes
Stub IP Multicast Routing	Yes
Security	
Additional Vendor-Proprietary RADIUS Attributes	Yes
Authenticating ACLs	Yes
Automated Double Authentication	Yes
HTTP Security	Yes
Named Method Lists for AAA Authorization & Accounting	Yes
Per User Configuration	Yes
Reflexive Access Lists	Yes
Vendor-Proprietary RADIUS Attributes	Yes
Switching	
Enhanced ATM VC Configuration and Management	Yes
Fastswitched Policy Routing	Yes
WAN Optimization	
DRP Server Agent Enhancement	Yes
PAD Subaddressing	Yes
WAN Services	
Bandwidth Allocation Control Protocol (BACP)	Yes
Dialer Watch	Yes
Enhanced Local Management Interface (ELMI)	Yes
Frame Relay Enhancements	Yes
Frame Relay MIB Extensions	Yes
Frame Relay Router ForeSight	Yes
MPPC-MS PPP Compression	Yes
MS Callback	Yes
Multiple ISDN Switch Type	Yes
National ISDN Switch Types	Yes
National ISDN Switch Types	Yes
X.25 Switching between PVCs and SVCs	Yes

Optional feature set licenses for the Cisco uBR7246 universal broadband routers are as follows:

- WAN Packet Protocols
 - ATM DXI

- Frame Relay switching
- Frame Relay SVC support (DTE)
- Frame Relay traffic shaping
- SMDS over ATM
- X.25
- X.25 switching
- Interdomain Routing
 - BGP
 - BGP4—Includes soft configuration, multipath support, and prefix filtering with inbound route maps
 - EGP for Internet scale routing

New and Changed Information

This section lists some of the features available for the Cisco uBR7200 series in Cisco IOS Release 12.0 software. For more information about these features, refer to the cross-platform *Release Notes for Cisco IOS Release 12.0* located on CCO and the Documentation CD-ROM.

- Additional Vendor-Proprietary RADIUS Attributes
- Automated Double Authentication
- Dialer Watch
- Microsoft Point-to-Point Compression (MPPC)
- MS Callback
- Multiple ISDN Switch Types
- Named Method Lists for AAA Authorization and Accounting
- National ISDN Switch Types
- VPDN MIB and Syslog Facility

Important Notes

This section contains important information about using Cisco IOS Release 12.0 software that might apply to Cisco uBR7200 series universal broadband routers.

- cable spectrum-group shared Command Not Supported, page 8
- Cisco IOS Syslog Failure, page 8
- Deprecated MIBs, page 13

cable spectrum-group shared Command Not Supported

The **cable spectrum-group shared** command was documented in the feature module *Cisco uBR7246 Universal Broadband Router Enhancements*, released with Cisco IOS Release 11.3(5)NA. This command is *not* supported on the Cisco uBR7246 at this time, and has *not* been supported in any previous release. It is scheduled to be supported beginning with Release 12.0(4)T.

cable spectrum-group shared

To specify that the upstream ports share the same spectrum, use the **cable spectrum-group shared** global configuration command. Use the **no** form of this command to delete the spectrum group.

This is *not* currently supported. In the meantime, if it is necessary to configure two upstream channels to share the same spectrum-group but have different frequencies, they can be configured manually.

As an example, you have two nodes with two upstream channels per node. Node one carries US0 and US1; node two carries US2 and US3. Assume also that you are allocated 25 MHz to 35 MHz for the two upstreams combined.

First, set up two spectrum groups:

```
cable spectrum-group 1 band 25000000 30000000
cable spectrum-group 2 band 30000000 35000000
```

Note Be sure you do not configure overlapping spectrum groups.

Then, allocate one channel from each node to each spectrum group:

```
cable us0 spectrum-group 1
cable us1 spectrum-group 2
cable us2 spectrum-group 1
cable us3 spectrum-group 2
```

Cisco IOS Syslog Failure

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

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

Assume that any potential attacker is likely to know that 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/iossyslog-pub.shtml>

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

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

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 5, *Affected and Repaired Software Versions*. 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 and will correct it in future maintenance and interim releases. See Table 5, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic 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 issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

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

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this 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

Important Notes

- 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 4 gives Cisco’s projected fix dates.

Make sure your hardware had 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 (say, from 11.2(11)P to 11.2(17)P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

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

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

<http://www.cisco.com>

If you have service contracts you can obtain new software through your regular update channels (generally via 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 don’t have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single 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. Non-contract customers must request free updates through the TAC. Please do not contact either “psirt@cisco.com” or “security-alert@cisco.com” for software updates.

Workarounds

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

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

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

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

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this 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 may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Important Notes

Software Versions and Fixes

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

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

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

Table 5 specifies information about affected and repaired software versions.

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—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))

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(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches.	Unaffected; one-time release	Unaffected	Unaffected; general upgrade path is via 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 and/or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 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, 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 may contain serious bugs.
- 3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
- 4 All dates in this table are estimates, subject to change.
- 5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release in which the vulnerability is fixed.

Deprecated MIBs

Older Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs, without affecting existing Cisco IOS products or NMS applications. Application developers should update from deprecated MIBs to the replacement MIBs as shown in the following table.

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)

Table 6 **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
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

For information on caveats in Cisco IOS Release 12.0, refer to the *Caveats for Cisco IOS Release 12.0* document. This caveats document lists severity 1 and 2 caveats for Release 12.0. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Caveats describe unexpected behavior or defects in Cisco IOS software releases.

This document is located on CCO and the Documentation CD-ROM.

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

Related Documentation

The following sections describe the documentation available for the Cisco uBR7200 series routers. Typically, these documents consist of hardware installation guides, software installation guides, Cisco IOS configuration and command references, system error messages, and feature modules, which are updates to the Cisco IOS documentation. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online only.

The most up-to-date documentation can be found on CCO and the Documentation CD-ROM. These electronic documents might contain updates and modifications made after the hard copy documents were printed.

These release notes should be used in conjunction with the documents listed in these sections.

- Release-Specific Documentation, page 15
- Platform-Specific Documents, page 15
- Cisco IOS Software Documentation Set, page 16

Release-Specific Documentation

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

- *Release Notes for Cisco IOS Release 12.0*

To reach the cross-platform *Release Notes for Cisco IOS Release 12.0* from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross Platform Release Notes

To reach the cross-platform *Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, click on this path:

Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross Platform Release Notes

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

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

Service & Support: Technical Documents

- Caveat document

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

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

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

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

Cisco IOS Software Configuration: Cisco IOS 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. From CCO, login and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

The documents listed in this section are available for the Cisco uBR7200 series. These documents are also available on CCO and the Documentation CD-ROM.

- *Cisco uBR7246 Installation and Configuration Guide*
- *Cisco uBR7223 Installation and Configuration Guide*
- Cisco uBR7200 Series Configuration Notes
- Cisco Network Registrar for the uBR7200 Series
- Regulatory and Safety Compliance for the Cisco uBR7246
- Regulatory and Safety Compliance for the Cisco uBR7223
- Cisco uBR7200 Series Universal Broadband Router Features

To access Cisco uBR7200 documentation on CCO, follow this path:

Service & Support: Documentation Home Page: Broadband/Cable Solutions: Cisco uBR7200 Series Universal Broadband Routers

To access Cisco uBR7200 documentation on the Documentation CD-ROM, follow this path:

Broadband/Cable Solutions: Cisco uBR7200 Series Universal Broadband Routers

Cisco IOS Software Documentation Set

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

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Each configuration guide can be used in conjunction with its corresponding command reference.

To reach these documentation modules on CCO, follow this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Cisco IOS Release 12.0 Configuration Guides and Command References

To reach these documentation modules on the Documentation CD-ROM, follow this path:

Cisco IOS Software Configuration: Cisco IOS Release 12.0: Cisco IOS Release 12.0 Configuration Guides and Command References

Release 12.0 Documentation Set

Table 7 details the contents of the Cisco IOS Release 12.0 software documentation set. The document set is available in electronic form, and also in printed form upon request.

Note The most current Cisco IOS documentation can be found on CCO and the Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed.

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

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

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

Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 7 Cisco IOS Software Documentation Set for Release 12.0

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
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>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

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

Books	Chapter Topics
<ul style="list-style-type: none">• <i>Cisco IOS Switching Services Configuration Guide</i>• <i>Cisco IOS Switching Services Command Reference</i>	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none">• <i>Wide-Area Networking Configuration Guide</i>• <i>Wide-Area Networking Command Reference</i>	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none">• <i>Voice, Video, and Home Applications Configuration Guide</i>• <i>Voice, Video, and Home Applications Command Reference</i>	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
<ul style="list-style-type: none">• <i>Quality of Service Solutions Configuration Guide</i>• <i>Quality of Service Solutions Command Reference</i>	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none">• <i>Cisco IOS Software Command Summary</i>• <i>Dial Solutions Quick Configuration Guide</i>• <i>System Error Messages</i>• <i>Debug Command Reference</i>	

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

Service and Support

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

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

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

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

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

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

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

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to provide notification of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects
- Hardware—Technical Tips related to specific hardware platforms
- Hot Tips—Popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC FAX-on-demand service. To reach FAX-on-demand and receive documents at your FAX machine from the USA, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Tips on using and deploying Cisco IOS software features and services
- Sample Configurations—Actual configuration examples—examples complete with topology and annotations
- Software Products—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations
- Special Collections—Other Helpful Documents, including Case Studies, References & 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 access 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 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 mentioned in the "Related Documentation" section on page 14.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, the CCIE logo, CCNA, CCNP, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, the Cisco Technologies logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetRanger Director, NetRanger Sensor, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratm, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, 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 BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, LightSwitch, MICA, Phase/IP, Registrar, StrataSphere, StrataView Plus, and SwitchProbe 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. (9901R)

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