



Text Part Number: 78-6383-02

# Release Notes for the Cisco 805 Router for Cisco IOS Release 12.0(4)XM

---

**February 15, 2002**

These release notes describe new features and significant software components for the Cisco 805 router supported by Cisco IOS Release 12.0(4)XM and Release 12.0(4)XM1. Use these release notes with the Cross-Platform Release Notes for Cisco IOS Release 12.0 T located on CCO and the Documentation CD-ROM.



**Caution** Cisco IOS Release 12.0(4)XM and above do not support Cisco 801, 802, 803, or 804 routers.

For a list of the software caveats that apply to Release 12.0(4)XM1, refer to the Caveats for Cisco IOS Release 12.0 T document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

## Contents

These release notes discuss the following topics:

- System Requirements, page 2
- New and Changed Information, page 7
- Important Notes, page 8
- Caveats, page 13
- Resolved 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 © 2002  
Cisco Systems, Inc.  
All rights reserved.

## System Requirements

This section describes the system requirements and includes the following sections:

- Memory Requirements, page 2
- Cisco 805 Routers, page 2
- Determining Your Software Release, page 3
- Upgrading to a New Software Release, page 3
- Cisco IOS Feature Sets for the Cisco 805 Router, page 3
- Feature Set Tables, page 4

## Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.0(4)XM1 on the Cisco 805 router.

**Table 1 Release 12.0(4)XM1 Memory Requirements for the Cisco 805 Router**

Platform/Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From
IP	c805-y6-mw	4 MB Flash	8 MB DRAM	RAM
IP Plus	c805-sy6-mw	4 MB Flash	8 MB DRAM	RAM
IP/IPX Plus	c805-nsy6-mw	4 MB Flash	8 MB DRAM	RAM
IP Firewall	c805-oy6-mw	4 MB Flash	8 MB DRAM	RAM

## Cisco 805 Routers

The Cisco 805 router connects small professional offices over serial lines to corporate networks and to the Internet. Table 2 summarizes Cisco 805 router ports.

**Table 2 Cisco 805 Router Ports**

<b>Ethernet Port</b>	One 10BaseT (RJ-45)
<b>Serial Port</b>	One WAN interface (RS-232, RS-449, RS-530 and RS-530A, V.35, and X.21)
<b>Console Port</b>	RJ-45

The Cisco 805 router provides the following key features:

- One serial WAN interface that delivers up to 512 kbps for synchronous serial connections (Frame Relay, leased lines, and X.25) or up to 115 kbps for asynchronous dial-up.
- One Ethernet LAN interface.
- Flash memory: 4 MB default, expandable to 12 MB.
- Dynamic RAM: 8 MB, expandable to 16 MB.
- Color-coded ports and cable reduce the chance of cabling errors.
- Routers can be stacked.

## Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 805 router, log in to the Cisco 805 router and enter the **show version EXEC** command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) c805 Software (c805-y6-mw), Version 12.0(4)XM1, 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 Software 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>

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 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99) product bulletin located on CCO.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under Cisco IOS12.0, click Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99).

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.

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

On CCO, click on this path:

Service & Support: Product Bulletins: Software

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

## Cisco IOS Feature Sets for the Cisco 805 Router

The following list shows which feature sets are supported on the Cisco 805 router. These feature sets only apply to Cisco IOS Release 12.0(4)XM1:

- IP
- IP Plus
- IP/IPX Plus
- IP/Firewall

## 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.



**Caution** Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 3 lists the features and feature sets supported by the Cisco 805 router in Cisco IOS Release 12.0(4)XM1 and uses the following conventions:

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

**Note** The Cisco 800 family runs a subset of the Cisco IOS commands that might be available on other hardware platforms. The following table is not a cumulative or complete list of all the features in each image.

**Table 3 Cisco IOS Software Feature Sets for the Cisco 805 Router**

Features	Feature Set			
	IP	IP Plus	IP/IPX Plus	IP Firewall
<b>Address Conservation</b>				
PAT (NAT Overload)	Yes	Yes	Yes	Yes
NAT (Network Address Translation)	Yes	Yes	Yes	Yes
NAT with H.323	No	No	No	No
PAT (Port Address Translation)	Yes	Yes	Yes	Yes
<b>Asynchronous</b>				
Chat Scripts	Yes	Yes	Yes	Yes
Reverse Telenet	Yes	Yes	Yes	Yes
<b>Ease of Use and Deployment</b>				
Auto Install Frame Relay	Yes	Yes	Yes	Yes
Cisco ConfigMaker	Yes	Yes	Yes	Yes
Cisco Fast Step	Yes	Yes	Yes	Yes
Configuration Express	Yes	Yes	Yes	Yes
Easy IP—Phase I and II (IPCP Address Negotiation and DHCP Server)	Yes	Yes	Yes	Yes
TFTP (Client and Server)	Yes	Yes	Yes	Yes

**Table 3 Cisco IOS Software Feature Sets for the Cisco 805 Router**

Features	Feature Set			
	IP	IP Plus	IP/IPX Plus	IP Firewall
<b>LAN</b>				
AppleTalk	No	No	No	No
IP	Yes	Yes	Yes	Yes
IPX	No	No	Yes	No
NetBIOS Access Lists	Yes	Yes	Yes	Yes
Transparent Bridging	Yes	Yes	Yes	Yes
<b>Management</b>				
CiscoView™	Yes	Yes	Yes	Yes
SNMP, Telnet, Console Port	Yes	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes
Syslog	No	Yes	Yes	No
<b>Routing</b>				
BGP	No	No	No	No
EGP	No	No	No	No
IGRP	No	No	No	No
IP Enhanced IGRP (IP-EIGRP)	No	Yes	Yes	No
IP Multicast (relay only)	No	Yes	Yes	No
IP-Policy Routing	No	Yes	Yes	No
IPX Enhanced IGRP (IPX-EIGRP)	No	No	No	No
IPXWAN	No	No	Yes	No
OSPF	No	No	No	No
RIP, RIPv2, Triggered RIP	Yes	Yes	Yes	Yes
Weighted Fair Queuing	Yes	Yes	Yes	Yes
<b>Security</b>				
AAA Radius	No	No	No	No
AAA TACACS+	No	No	No	No
Access Control Lists	Yes	Yes	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes	No	No	No	No
Authenticating ACL	No	No	No	No
Automated Double Authentication (server functionality)	No	No	No	No
Certificate Authority Interoperability	No	No	No	No
GRE Tunneling	No	Yes	Yes	No
Internet Key Exchange Security Protocol	No	No	No	No
IPSec Network Security	No	No	No	No

## System Requirements

**Table 3 Cisco IOS Software Feature Sets for the Cisco 805 Router**

Features	Feature Set			
	IP	IP Plus	IP/IPX Plus	IP Firewall
<b>IOS Firewall — Phase I</b>				
— Context-based Access Control Lists	No	No	No	Yes
— Denial-of-service Protection and Prevention	No	No	No	Yes
— Java Blocking	No	No	No	Yes
— Real-time Alerts and Audit Trails	No	No	No	Yes
IPSec Encryption with 56 bit DES	No	No	No	No
Lock and Key	Yes	Yes	Yes	Yes
L2TP	No	No	No	No
Named Method Lists for AAA Authentication & Accounting	No	No	No	No
PAP, CHAP, MS-CHAP, Local Password	Yes	Yes	Yes	Yes
Route and Router Authentication	Yes	Yes	Yes	Yes
Token Card - Single Authentication	No	No	No	No
Token Card - Double Authentication	Yes	Yes	Yes	Yes
<b>WAN</b>				
Frame Relay Inverse ARP	Yes	Yes	Yes	Yes
Frame Relay PVC	Yes	Yes	Yes	Yes
Leased Lines	Yes	Yes	Yes	Yes
ML-PPP, PPP Compression	Yes	Yes	Yes	Yes
Mobile IP	No	No	No	No
PPP, HDLC, LAPB, SLIP	Yes	Yes	Yes	Yes
PPP over Frame Relay (RFC 1973)	No	No	No	No
Switched 56K	Yes	Yes	Yes	Yes
X.25	No	Yes	Yes	No
<b>WAN Optimization</b>				
Dial on Demand (DDR)	Yes	Yes	Yes	Yes
FR.9 Compression	Yes	Yes	Yes	Yes
HSRP	No	No	No	No
IPX and SPX Spoofing	No	No	Yes	No
RTP Header Compression	Yes	Yes	Yes	Yes
Snapshot Routing	Yes	Yes	Yes	Yes
STAC Compression	Yes	Yes	Yes	Yes
Time Based Access Lists	Yes	Yes	Yes	Yes
X.25 ID	No	Yes	Yes	No

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 805 router for Release 12.0(4)XM1.

### New Hardware Features in Release 12.0(4)XM

The following new hardware enhancements are supported by the Cisco 805 router for Release 12.0(4)XM and above. For more information about Cisco 805 router hardware, see the “Platform-Specific Documents” section on page 15.

#### Support for the Cisco 805 Router

Cisco IOS Release 12.0(4)XM includes support for the Cisco 805 router, which offers flexibility to small offices requiring secure and manageable Internet, intranet, and corporate LAN access. The Cisco 805 router has a fixed hardware configuration with one 10BaseT Ethernet port and one serial port. The serial port can connect X.21, V.35, RS-232, RS-449, RS-530 and RS-530A DTE and DCE.

### New Software Features in Release 12.0(4)XM

The following new software capabilities are supported by the Cisco 805 router for Release 12.0(4)XM.

- Software Support for the Cisco 805 Router
- Cisco IOS Firewall Feature Set for the Cisco 805 Router

#### Software Support for the Cisco 805 Router

Cisco IOS Release 12.0(4)XM provides support for the Cisco 805 router.



**Caution** The Cisco 805 router runs Cisco IOS Release 12.0(4)XM and above only. Cisco IOS Release 12.0(4)XM and above do not support Cisco 801, 802, 803, or 804 routers.

#### Cisco IOS Firewall Feature Set for the Cisco 805 Router

The Cisco IOS Firewall feature set is now available on the Cisco 805 router. This feature set is available on the IP Firewall image only; the product code for this image is S805C-12.0.4XM. This feature set provides the following capabilities:

- Context-based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The *Cisco IOS Firewall Feature Set* feature module provides several sample firewall configurations, including the following examples for small-office environments:

- IP network to Internet
- Remote office network to corporate office network

If you want to configure a firewall in an IP-network-to-Internet network, you can use the Cisco 805 series Fast Step application (recommended for inexperienced network administrators) or the Cisco IOS software command-line interface (CLI) (recommended for more experienced network administrators). You can also configure a firewall by using Cisco ConfigMaker software version 2.3.

With the Cisco 805 Fast Step application, you can configure CBAC only. If you want to configure a firewall in a remote-office-to-corporate-office network, you must use the Cisco IOS CLI.

For information on how to use the Cisco 805 Fast Step application, refer to the application online help. For information on how to configure a firewall using the CLI, refer to the *Cisco IOS Firewall Feature Set* feature module.

## Important Notes

This section contains the following important notes about Cisco IOS Release 12.0(4)XM1 that apply to the Cisco 805 router:

- Maximum Speed for Cisco 805 Router Synchronous Interfaces
- Cisco IOS Syslog Failure

### Maximum Speed for Cisco 805 Router Synchronous Interfaces

The Cisco 805 router limits the maximum operating speed of synchronous interfaces to a maximum of 512 K in both DTE mode and DCE mode. When the Cisco 805 router is in DTE mode and the clock rate exceeds 512 K, the serial link is shut down and the following message appears on the console:

```
WARNING:MAXIMUM INTERFACE SPEED OF 512KB EXCEEDED  
SHUTTING DOWN INTERFACE.
```

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

### Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 4, 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 4. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 4, 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 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 (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 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 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 4, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

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

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either “[psirt@cisco.com](mailto:psirt@cisco.com)” or “[security-alert@cisco.com](mailto: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 by 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 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 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 Cisco IOS 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 Release 12.0 mainline software is Release 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

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

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

Table 4 specifies information about affected and repaired software versions.

---

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

---

**Table 4** Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix <sup>1</sup>	First Fixed Interim Release <sup>2</sup>	Fixed Maintenance Release <sup>3</sup>
<b>Unaffected Releases</b>				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
<b>Releases Based on 11.3</b>				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 <sup>4</sup>	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
<b>Releases Based on 12.0</b>				
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 <sup>5</sup> , 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 4** Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix <sup>1</sup>	First Fixed Interim Release <sup>2</sup>	Fixed Maintenance Release <sup>3</sup>
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 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.

## Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. All caveats in Release 12.0 and 12.0 T are also in Release 12.0(4)XM1.

For information on caveats in Cisco IOS Release 12.0 T, refer to the *Caveats for Cisco IOS Release 12.0 T* document. For information on caveats in Cisco IOS Release 12.0, refer to the *Caveats for Cisco IOS Release 12.0* document. Both of these documents list severity 1 and 2 caveats and are located on CCO and the Documentation CD-ROM.

---

**Note** If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

---

## Resolved Caveats

### Cisco IOS Release 12.0(4)XM1

Cisco IOS Release 12.0(4)XM1 is a rebuild of Cisco IOS Release 12.0(4)XM. All caveats in this section have been resolved in Cisco IOS Release 12.0(4)XM1 but may be open in previous Cisco IOS releases.

- CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

## Related Documentation

The following sections describe the documentation available for the Cisco 805 router. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 14
- Platform-Specific Documents, page 15
- Feature Modules, page 15
- Cisco IOS Software Documentation Set, page 16

## Release-Specific Documents

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 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

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

**Service & Support: Technical Documents**

- *Caveats for Cisco IOS Release 12.0 T*

For a list of the Release 12.0 and 12.0 T caveats related to Release 12.0(4)XM1, see the *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contain caveats applicable to all platforms.

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

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

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

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

---

**Note** If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

---

## Platform-Specific Documents

These documents are available for the Cisco 805 router on CCO and the Documentation CD-ROM.

- *Cisco 805 Router Hardware Installation Guide*
- *Quick Start Guide — Setting up the Cisco 805 Router*
- *Regulatory Compliance and Safety Info For the Cisco 805 Router*
- *Cisco 805 Router Software Configuration Guide*
- *Release Notes for the Cisco 805 Router*

To reach Cisco 805 router documentation from CCO, click on this path:

**Service & Support: Documentation Home Page: Access Servers and Access Routers: Fixed Access Routers: Cisco 805 Router**

To reach Cisco 805 router documentation on the Documentation CD-ROM, click on this path:

**Cisco Product Documentation: Access Servers and Access Routers: Fixed Access Routers: Cisco 805 Router**

## Feature Modules

Feature modules describe new features supported by Release 12.0 T 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.

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

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

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

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

## Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to set up an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. 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 they contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

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

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

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

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

## Release 12.0 Documentation Set

Table 5 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.

---

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

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

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

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

**Table 5 Cisco IOS Software Release 12.0 Documentation Set**

<b>Books</b>	<b>Chapter Topics</b>
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview

**Table 5 Cisco IOS Software Release 12.0 Documentation Set (continued)**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	<ul style="list-style-type: none"> <li>IP Addressing</li> <li>IP Services</li> <li>IP Routing Protocols</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	<ul style="list-style-type: none"> <li>AppleTalk</li> <li>Novell IPX</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	<ul style="list-style-type: none"> <li>Apollo Domain</li> <li>Banyan VINES</li> <li>DECnet</li> <li>ISO CLNS</li> <li>XNS</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>AAA Security Services</li> <li>Security Server Protocols</li> <li>Traffic Filtering and Firewalls</li> <li>IP Security and Encryption</li> <li>Passwords and Privileges</li> <li>Neighbor Router Authentication</li> <li>IP Security Options</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Switching Paths for IP Networks</li> <li>Virtual LAN (VLAN) Switching and Routing</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>ATM</li> <li>Frame Relay</li> <li>SMDS</li> <li>X.25 and LAPB</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Voice over IP</li> <li>Voice over Frame Relay</li> <li>Voice over ATM</li> <li>Voice over HDLC</li> <li>Video Support</li> <li>Universal Broadband Features</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Classification</li> <li>Scheduling</li> <li>Packet Drop</li> <li>Traffic Shaping</li> <li>ATM QoS</li> <li>SNA QoS</li> <li>Line Protocols</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

---

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

---

## Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs that are described in the “Service and Support” section of the *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 helpful tips on configuring your Cisco products:

[http://www.cisco.com/kobayashi/serv\\_tips.shtml](http://www.cisco.com/kobayashi/serv_tips.shtml)

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

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Collection of the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—Popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

## Cisco Connection Online

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

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Toolkit, 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](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](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

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

---

## Documentation CD-ROM

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

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

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 14.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

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