



Release Notes for Cisco 800 Series for Cisco IOS Release 12.0 T

December 13, 1999

These release notes for Cisco 800 series support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(7)T, see 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.

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



Note

Cisco IOS Release 12.0(5)T and earlier support the Cisco 801–804 only. The Cisco 805 router was introduced in the latest release, Release 12.0(7)T.

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 12
- Important Notes, page 20
- Caveats, page 27
- Related Documentation, page 29
- Obtaining Documentation, page 34
- Obtaining Technical Assistance, page 35



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

Copyright © 1999–2000. Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 2
- Hardware Supported, page 2
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for the Cisco 800 Series

Platforms	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs From
Cisco 801–804 Routers	IP	c800-y6-mw	8 MB	4 MB	RAM
	IP Plus	c800-sy6-mw	8 MB	4 MB	RAM
	IP/IPX Plus	c800-nsy6-mw	8 MB	4 MB	RAM
	IP/Firewall	c800-oy6-mw	8 MB	4 MB	RAM
	IP/Firewall Plus	c800-osy6-mw	8 MB	4 MB	RAM
	IP/FW/Plus/IPSEC56	c800-osy656i-mw	8 MB	8 MB	RAM
	IP/IPX/FW/IPSEC56/Plus	c800-nosy656i-mw	8 MB	8 MB	RAM
Cisco 805 Router	IP	c805-y6-mw	4 MB	8 MB	RAM
	IP Plus	c805-sy6-mw	4 MB	8 MB	RAM
	IP/IPX Plus	c805-nsy6-mw	4 MB	8 MB	RAM
	IP/Firewall	c805-oy6-mw	4 MB	8 MB	RAM
	IP/Firewall Plus	c805-osy6-mw	4 MB	4 MB	RAM
	IP/FW/Plus/IPSEC56	c805-osy656i-mw	8 MB	8 MB	RAM
	IP/IPX/FW/IPSEC56/Plus	c805-nosy656i-mw	8 MB	8 MB	RAM

Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 800 series:

- Cisco 801
- Cisco 802
- Cisco 803
- Cisco 804
- Cisco 805

**Note**

Cisco IOS Release 12.0(5)T and earlier support the Cisco 801–804 only. The Cisco 805 router was introduced in the latest release, Release 12.0(7)T.

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 12.

Table 2 Supported Interfaces for the Cisco 800 Series

Router	Ethernet Ports	ISDN Ports	Serial Ports	Telephone Ports	Console Ports
Cisco 801	One 10BaseT (RJ-45)	ISDN BRI S/T (RJ-45)	–	–	RJ-45
Cisco 802	One 10BaseT (RJ-45)	ISDN BRI U, integrated Network Termination 1 (NT-1) (RJ-45)	–	–	RJ-45
Cisco 803	Four-port 10BaseT (RJ-45) hub	ISDN BRI S/T (RJ-45)	–	Two (RJ-11)	RJ-45
Cisco 804	Four-port 10BaseT (RJ-45) hub	ISDN BRI U, integrated NT-1 (RJ-45)	–	Two (RJ-11)	RJ-45
Cisco 805	One 10BaseT (RJ-45)	–	One smart serial (RS-232, RS-449, RS-530, RS-530A, X.21 and V.35)	–	RJ-45

Cisco 801–804 Routers

The Cisco 801–804 routers provide the following key hardware features:

- Cisco 802 and Cisco 804 routers have an integrated NT-1, which eliminates the need for an external NT-1 in North America.
- Cisco 803 and Cisco 804 routers provide connection to analog telephones, fax machines, or modems, which are connected to telephone services through an ISDN line.
- Flash memory: Default is 8 MB, expandable to 12 MB. (4MB Flash soldered to the motherboard.)

**Note**

To add additional Flash memory to the Cisco 801-804, you will remove the existing Flash card and install a the new one.

- Dynamic RAM: Default is 4 MB, expandable to 12 MB. (4MB Dynamic RAM soldered to the motherboard.)
- ISDN B-channel LEDs are a different color from the other LEDs, which make them easy to distinguish.
- Color-coded ports and cable reduce the chance of cabling errors.
- Routers can be stacked or mounted on a wall.

Cisco 805 Router

The Cisco 805 router connects small professional offices over serial lines to corporate networks and to the Internet, and 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: Default is 4 MB, expandable to 12 MB. (4MB Flash soldered to the motherboard.)
- Dynamic RAM: Default is 8 MB, expandable to 16 MB. (8 MB Dynamic RAM soldered to the motherboard.)
- Color-coded ports and cable reduce the chance of cabling errors.
- Routers can be stacked.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 800 series, log in to the router and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 800 Software (C800-Y6-MW), Version 12.0(7)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

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

Technical Documents: Product Bulletins: Software

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

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 800 series.

Table 3 Feature Sets Supported by the Cisco 800 Series

Image Names	Feature Set Matrix Term	Software Image	Platforms	In ¹
IP	Basic ²	c800-y6-mw	Cisco 801–804	
		c805-y6-mw	Cisco 805	(7)
IP Plus	Plus ³	c800-sy6-mw	Cisco 801–804	
		c805-sy6-mw	Cisco 805	(7)
IP/IPX Plus	Plus	c800-nsy6-mw	Cisco 801–804	
		c805-nsy6-mw	Cisco 805	(7)
IP/Firewall	Basic	c800-oy6-mw	Cisco 801–804	
		c805-oy6-mw	Cisco 805	(7)
IP/Firewall Plus	Plus	c800-osy6-mz	Cisco 801–804	(5)
		c805-osy6-mz	Cisco 805	(7)
IP/FW/Plus/IPSEC56	Plus, IPsec 56 ⁴	c800-osy656i-mw	Cisco 801–804	(5)
		c805-osy656i-mw	Cisco 805	(7)
IP/IPX/FW/IPSEC56/Plus	Plus, IPsec 56	c800-nosy656i-mw	Cisco 801–804	(5)
		c805-nosy656i-mw	Cisco 805	(7)

1. The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.
2. This feature set is offered in the basic feature set.
3. This feature set is offered in the Plus feature set.
4. This feature set is offered in the encryption feature sets, which consist of IPsec 56-bit (Plus IPsec 56) data encryption feature sets.

**Caution**

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

Table 4 and Table 5 list the features and feature sets supported by the Cisco 801–804 routers in Cisco IOS Release 12.0 T, and Table 6 lists the features and feature sets supported by the Cisco 805 router. All three tables use the following conventions:

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

**Note**

These feature set tables only contain a selected list of features. These tables are not cumulative—nor do they list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 801–804 Routers

Features	Feature Set							
	In	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/ IPSEC56 (VPN)	IP/IPX/FW/ IPSEC56/ Plus
Address Conservation								
PAT (NAT Overload)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT		Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT with H.323		No	No	No	No	No	No	No
Advanced Telephone Features¹								
Call Forward (Sweden and Finland only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call Forward Variable (North America only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call Hold Retrieve (North America only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call Transfer (North America only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call Waiting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Caller ID Number delivery to POTS ports (North America only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Caller ID Name delivery to POTS ports (North America only)		No	No	No	No	No	No	No
Data-Over-Voice Bearer (North America only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Distinctive Ringing		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN-Voice Priority		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Basic Services								
GRE Tunneling		No	Yes	Yes	No	Yes	Yes	Yes
NAT		Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAP, CHAP, MSCHAP, Local Password		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ease of Use and Deployment								
Auto SPID / Switch Detection	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco ConfigMaker		Yes	Yes	Yes ²	Yes	Yes	Yes	Yes
Cisco FastStep		Yes	Yes	Yes ²	Yes	Yes	Yes	Yes
Easy IP Phase I and II (IPCP Address Negotiation and DHCP Server)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TFTP Client and Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 801–804 Routers (continued)

Features	Feature Set							
	In	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/ IPSEC56 (VPN)	IP/IPX/FW/ IPSEC56/ Plus
LAN								
AppleTalk		No	No	No	No	No	No	No
IP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX		No	No	Yes	No	No	No	Yes
NetBIOS Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent Bridging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management								
Cisco View		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP, Telnet, Console Port		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNTP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Syslog		No	Yes	Yes	No	Yes	Yes	Yes
Routing								
BGP		No	No	No	No	No	No	No
EGP		No	No	No	No	No	No	No
IGRP		No	No	No	No	No	No	No
IP Enhanced IGRP (IP-EIGRP)		No	Yes	Yes	No	Yes	Yes	Yes
IPX Enhanced IGRP (IPX-EIGRP)		No	No	No	No	No	No	No
IP Multicast (relay only)		No	Yes	Yes	No	Yes	Yes	Yes
IP-Policy Routing		No	Yes	Yes	No	Yes	Yes	Yes
IPXWAN		No	No	Yes	No	No	No	Yes
OSPF		No	No	No	No	No	No	No
RIP, RIPv2, Triggered RIP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security								
AAA Radius		No	No	No	No	No	No	No
AAA TACACS+		No	Yes	Yes	No	Yes	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes		No	No	No	No	No	No	No
Authenticating ACL		No	No	No	No	No	No	No
Automated Double Authentication (server functionality)		No	No	No	No	No	No	No
Certificate Authority Interoperability ³		No	No	No	No	No	Yes	Yes
Internet Key Exchange Security Protocol		No	No	No	No	No	Yes	Yes
IPSec Network Security	(5)	No	No	No	No	No	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 801–804 Routers (continued)

Features	Feature Set							
	In	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/ IPSEC56 (VPN)	IP/IPX/FW/ IPSEC56/ Plus
IOS Firewall Phase I								
– Context Based Access Control Lists		No	No	No	Yes	Yes	Yes	Yes
– Java Blocking		No	No	No	Yes	Yes	Yes	Yes
– Denial of Service Detection and Prevention		No	No	No	Yes	Yes	Yes	Yes
– Real-time Alerts and Audit Trails		No	No	No	Yes	Yes	Yes	Yes
IPSec Encryption with 56 bit DES		No	No	No	No	No	Yes	Yes
Lock and Key		Yes	Yes	Yes	Yes	Yes	Yes	Yes
LT2P		No	No	No	No	No	Yes	Yes
Named Method Lists for AAA Authentication & Accounting		No	No	No	No	No	No	No
Route and Router Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Token Card - Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice Technologies								
Called Party Number Port	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN								
Frame Relay Encapsulation (for ISDN LL)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Digital Subscriber Line (IDSL, up to 144 kbps) (Cisco 802 & Cisco 804 only)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Digital Subscriber Line (IDSL)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Inverse ARP		No	No	No	No	No	No	No
ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Leased Line (up to 144 kbps)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ML-PPP, PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP		No	No	No	No	No	No	No
PPP over Frame Relay (RFC 1973)		No	No	No	No	No	No	No
WAN Optimization								
Always On/Dynamic ISDN (AO/DI)		No	Yes	Yes	No	Yes	Yes	Yes
Bandwidth on Demand (BOD)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dial on Demand (DDR)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
HSRP		No	No	No	No	No	No	No

Table 4 Feature List by Feature Set for the Cisco 801–804 Routers (continued)

Features	Feature Set							
	In	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/IPSEC56 (VPN)	IP/IPX/FW/IPSEC56/Plus
IPX and SPX Spoofing		No	No	Yes	No	No	No	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Snapshot Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stac Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-based Access Lists	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 ID		No	Yes	Yes	No	Yes	Yes	Yes

- Advanced Telephone Features are available on the Cisco 803 and 804 routers only. These features require supplementary services from a telephone company.
- The X.25 configuration feature requires the use of the Cisco command line interface (CLI).
- Interoperability with Certification Authority servers from VeriSign is not supported for IPsec in Release 12.0(5)T and earlier releases on Cisco 800 series routers.

The Cisco 800 series routers also support the features listed in Table 5.

Table 5 Additional Features supported by Cisco 800 Routers

Feature	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/IPSec	IP/FW/Plus/IPSec Plus
Routed Protocol	IP	IP	IP/IPX	IP	IP	IP	IP/IPX
Routing Protocol	RIP Snapshot	RIP/IP- EIGRP Snapshot	RIP/IP- EIGRP/IPX WAN Snapshot	RIP/IP- EIGRP Snapshot	RIP/IP- EIGRP Snapshot	RIP/IP- EIGRP Snapshot	RIP/IP- EIGRP/IPX WAN Snapshot
Tunneling		GRE	GRE		GRE	GRE	GRE
X.25		X.25	X.25		X.25	X.25	X.25
SNTP (Simple Network Time Protocol)	SNTP	SNTP	SNTP	SNTP	SNTP	SNTP	SNTP
Multicast		IP Multicast Forwarding	IP Multicast Forwarding		IP Multicast Forwarding	IP Multicast Forwarding	IP Multicast Forwarding
Management	SNMP	SNMP/ SYSLOG	SNMP/ SYSLOG	SNMP	SNMP/ SYSLOG	SNMP/ SYSLOG	SNMP/ SYSLOG
Manual ISDN Calls (see reference for commands)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 805 Router

Features	Feature Set						
	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/ IPSEC56 (VPN)	IP/IPX/FW/ IPSEC56/ Plus
Address Conservation							
PAT (NAT Overload)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT with H.323	No	No	No	No	No	No	No
Basic Services							
GRE Tunneling	No	Yes	Yes	No	Yes	Yes	Yes
NAT	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAP, CHAP, MSCHAP, Local Password	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ease of Use and Deployment							
Cisco ConfigMaker	Yes	Yes	Yes ²	Yes	Yes	Yes	Yes
Cisco FastStep	Yes	Yes	Yes ¹	Yes	Yes	Yes	Yes
Easy IP Phase I and II (IPCP Address Negotiation and DHCP Server)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TFTP Client and Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN							
AppleTalk	No	No	No	No	No	No	No
IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX	No	No	Yes	No	No	No	Yes
NetBIOS Access Lists	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent Bridging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management							
Cisco View	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP, Telnet, Console Port	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Syslog	No	Yes	Yes	No	Yes	Yes	Yes
Routing							
BGP	No	No	No	No	No	No	No
EGP	No	No	No	No	No	No	No
IGRP	No	No	No	No	No	No	No
IP Enhanced IGRP (IP-EIGRP)	No	Yes	Yes	No	Yes	Yes	Yes
IPX Enhanced IGRP (IPX-EIGRP)	No	No	No	No	No	No	No
IP Multicast (relay only)	No	Yes	Yes	No	Yes	Yes	Yes
IP-Policy Routing	No	Yes	Yes	No	Yes	Yes	Yes
IPXWAN	No	No	Yes	No	No	No	Yes

Table 6 Feature List by Feature Set for the Cisco 805 Router (continued)

Features	Feature Set						
	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/ IPSEC56 (VPN)	IP/IPX/FW/ IPSEC56/ Plus
OSPF	No	No	No	No	No	No	No
RIP, RIPv2, Triggered RIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security							
AAA Radius	No	No	No	No	No	No	No
AAA TACACS+	No	Yes	Yes	No	Yes	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes	No	No	No	No	No	No	No
Authenticating ACL	No	No	No	No	No	No	No
Automated Double Authentication (server functionality)	No	No	No	No	No	No	No
Certificate Authority Interoperability	No	No	No	No	No	Yes	Yes
Internet Key Exchange Security Protocol	No	No	No	No	No	Yes	Yes
IPSec Network Security	No	No	No	No	No	Yes	Yes
IOS Firewall Phase I							
– Context Based Access Control Lists	No	No	No	Yes	Yes	Yes	Yes
– Java Blocking	No	No	No	Yes	Yes	Yes	Yes
– Denial of Service Detection and Prevention	No	No	No	Yes	Yes	Yes	Yes
– Real-time Alerts and Audit Trails	No	No	No	Yes	Yes	Yes	Yes
IPSec Encryption with 56 bit DES	No	No	No	No	No	Yes	Yes
Lock and Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LT2P	No	No	No	No	No	Yes	Yes
Named Method Lists for AAA Authentication & Accounting	No	No	No	No	No	No	No
Route and Router Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Token Card - Double Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN							
Frame Relay Encapsulation (for ISDN LL)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Inverse ARP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ML-PPP, PPP Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	No	No	No	No	No	No	No
PPP over Frame Relay (RFC 1973)	No	No	No	No	No	No	No
WAN Optimization							
Bandwidth on Demand (BOD)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dial on Demand (DDR)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 805 Router (continued)

Features	Feature Set						
	IP	IP Plus	IP/IPX Plus	IP/FW	IP/FW Plus	IP/FW/Plus/IPSEC56 (VPN)	IP/IPX/FW/IPSEC56/Plus
HSRP	No	No	No	No	No	No	No
IPX and SPX Spoofing	No	No	Yes	No	No	No	Yes
Snapshot Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stac Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-based Access Lists	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 ID	No	Yes	Yes	No	Yes	Yes	Yes

1. The X.25 configuration feature requires the use of the Cisco command line interface (CLI).

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 800 series for Release 12.0 T:

New Hardware Features in Release 12.0(7)T

The following new hardware feature is supported by the Cisco 800 series for Release 12.0(7)T and later releases:

Cisco 805 Router

Cisco IOS Release 12.0(7)T 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(7)T

The following new software enhancements are supported by the Cisco 800 series for Release 12.0(7)T and later releases:

TACACS+ on Cisco 800 Series Routers

Cisco 800 series routers now support the Terminal Access Controller Access Control System Plus (TACACS+) protocol through Telnet. TACACS+ is a Cisco proprietary authentication protocol that provides remote access authentication and related network security services, such as event logging. User passwords are administered in a central database rather than in individual routers.

The TACACS+ security application provides the centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon that typically runs on a UNIX or Windows NT workstation. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

The TACACS+ feature is supported by the authentication, authorization, and accounting (AAA) facility, which is configured at individual routers. However, Cisco 800 series routers do not support the RADIUS or Kerberos protocols. The TACACS+ AAA services are defined as follows:

Authentication--Provides complete control of authentication through login and password dialog, challenge and response, messaging support. The authentication facility provides the ability to conduct an arbitrary dialog with the user (for example, after a login and password are provided, to challenge a user with a number of questions, like home address, mother's maiden name, service type, and social security number. In addition, the TACACS+ authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of a company password aging policy.

Authorization--Provides fine-grained control over user capabilities for the duration of the a user session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.

Accounting--Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

For additional information, see and the *Cisco 800 Series Routers Software Configuration Guide*, *Cisco 805 Router Software Configuration Guide*, and the security-related configuration guides and command references located on CCO and the Documentation CD-ROM:

- To reach the *Cisco 800 Series Routers Software Configuration Guide* and *Cisco 805 Router Software Configuration Guide* from CCO, click on these paths:
 - **Service & Support: Documentation Home Page: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 801–804 Routers: Cisco 800 Series Routers Software Configuration Guide**
 - **Service & Support: Documentation Home Page: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 805 Router: Cisco 805 Router Software Configuration Guide**

- To reach the *Cisco 800 Series Routers Software Configuration Guide* and *Cisco 805 Router Software Configuration Guide* on the Documentation CD-ROM, click on these paths:
 - **Cisco Product Documentation: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 801–804 Routers: Cisco 800 Series Routers Software Configuration Guide**
 - **Cisco Product Documentation: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 805 Router: Cisco 805 Router Software Configuration Guide**
- To reach the security-related configuration guides and command references from CCO, click on these paths:
 - **Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Security Configuration Guide**
 - **Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Security Command Reference: Security Server Protocols: TACACS, Extended TACACS, and TACACS+ Commands**
- To reach the security-related configuration guides and command references on the Documentation CD-ROM, click on these paths:
 - **Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Security Configuration Guides**
 - **Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Security Command Reference: Security Server Protocols: TACACS, Extended TACACS, and TACACS+ Commands**

New Software Features in Release 12.0(5)T

The following new software enhancements are supported by the Cisco 800 series in Release 12.0(5)T and later releases.

Cisco IOS Firewall Feature Set for the Cisco 800 Series

Cisco IOS Firewall Feature Set is not new to Release 12.0(5)T; however, the Cisco IOS Firewall Feature Set combined with IPSEC is new to this release.

Enhancements to the Cisco IOS Firewall feature set are now available on the Cisco 800 series routers. This feature set is available on the IP Firewall, IP Firewall Plus, IP Firewall Plus IPsec, and IP/IPX Firewall Plus IPsec images only. This feature set provides the following additional capabilities:

- Context Based Access Control (CBAC)
- Java Blocking
- Denial of Service
- 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 800 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 800 Fast Step application, you can configure CBAC only. For information on how to use the Cisco 800 Fast Step application, refer to the application online help.

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 configure a firewall using the CLI, refer to the following online documents:

- *Cisco IOS Firewall Feature Set* feature module document
- *Security Configuration Guide*
- *Security Command Reference*

IPSec Network Security

The IPSec network security feature is now available on the Cisco 800 series routers (IP/Firewall/Plus/IPSec56 and IP/IPX/Firewall/IPSec56/Plus images only). This feature supports the 56-bit Data Encryption Standard (DES); it does not support the triple DES. Enabling this feature can impact your router performance.

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers, such as two routers. IPSec provides these security services on IP datagrams.

For information on configuring this feature, refer to the *Cisco IOS Release 12.0 Security Configuration Guide*.

Called Party Number Port

Some switches do not include a called party number when they send a voice call to a Cisco 800 router. These calls are directed to port 1 by default. The feature Called Party Number Port allows the router to direct calls of this type to a specified port. When this feature is combined with the command `forward-to-unused-port`, the router can direct a second call to the same port as the first call or to another port.

Layer Two Tunneling Protocol (L2TP)

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

Traditional dial-up networking services only supported registered IP address, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

New Software Features in Release 12.0(4)T

The following new software enhancements are supported by the Cisco 800 series in Release 12.0(4)T1 and later releases.

Cisco IOS Firewall Feature Set for the Cisco 800 Series

The Cisco IOS Firewall feature set is now available on the Cisco 800 series routers. This feature set is available on the IP/Firewall image only; the product code for this image is S8CH-12.0(4)T. 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 800 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 800 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 800 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. (See the “Feature Modules” section on page 31.)

Forwarding Incoming Call to Unused Port

A new command **forward-to-unused-port** has been added to the dial peer configuration. The default is **no forward-to-unused-port**.

- Behavior when forward-to-unused-port is set

Suppose a call to 555-1111 is received and its dial peer is fetched and this points to port 1. The following will determine where the new call will be forwarded:

- Case A:
Port 1 currently has no call on it. The new call to 555-1111 is sent to port 1.
- Case B:
Port 1 already has one call to 555-1111. The new call to 555-1111 is sent to port 1.
- Case C:
Port 1 has one call to 555-2222 and port 2 has no calls. The new call to 555-1111 is sent to port 2.
- Case D:
Port 1 has one call to 555-2222 and port 2 has one call to 555-1111. The new call to 555-1111 is sent to port 2.
- Case E:
Port 1 has one call to 555-2222 and port 2 has one call to 555-3333. The new call to 555-1111 is sent to port 1.
- Case F:
Port 1 has one call to 555-2222 and port 2 has two calls. The new call to 555-1111 is sent to port 1.
- Case G:
Port 1 already has 2 calls. The new call to 555-1111 is sent to port 2.

- Known problems

- Problem 1: DMS NI1 line with multiple numbers:

Suppose we have the following spids and dial peers:

```
isdn spid1 40855511110101 5551111 5552222
```

```
dial-peer v 1 p
destination-pattern 5551111
forward-to-unused-port
port 1
```

```
dial-peer v 2 p
destination-pattern 5552222
forward-to-unused-port
port 1
```

A call for 555-1111 is first received. So, it is connected to port 1. Then, a call to 555-2222 is received. Since port 2 has no calls, this new call is sent to port 2. The DMS NI1 will then release the second call because it is expecting the first call to be put on hold.

- Problem 2: No called party number is received

This new feature will work only if a called party number is received inside the incoming call. If no called part number is received then the incoming call will be directed to port 1.

Outgoing SPID Hunt

Outgoing hunt is a new pots feature on the Cisco 800 series. This feature is available for US switch types only. When enabled, the CSM will look for a free SPID to use for out going voice calls. If no calls are in progress then the SPID associated with the dial-peer destination is used. The customer must continue to program dial peers. By default, this feature is off.

Command syntax:

```
pots outgoing-hunt
no pots outgoing-hunt
```

New Features in Release 12.0(3)T

Cisco IOS Release 12.0(3)T was the first 12.0 T release to support Cisco 800 series routers.

The following new software enhancements, which were introduced in Release 12.0(1)T, are supported by the Cisco 800 series beginning in this release.

Voice Features Over ISDN

The Cisco 800 series routers support the connection of analog telephones, fax machines, and modems. These devices are connected to basic telephone services through the ISDN line. The routers support the following supplementary services, which can be ordered from the telephone service provider:

- Call holding and retrieving (North America only)
- Call waiting (North America only)
- Three-way call conferencing (North America only)
- Call transferring (North America only)
- Call forwarding (Sweden and Finland only)

The ISDN voice priority feature controls the priority of data and voice calls for the devices connected to the router telephone ports. If an ISDN circuit endpoint is busy with a data call or calls, and either a voice call comes in or you attempt to place a voice call, the data call is handled per the voice priority setting.

Automatic Detection of ISDN Switch and SPIDs

This feature applies to North America only. The Cisco 800 series routers can detect the ISDN switch that supports the ISDN line and the service profile identifiers (SPIDs) assigned by the telephone service provider. SPIDs identify the ISDN B channels. The SPID format is generally an ISDN telephone number with numbers added to it, for example, 40855522220101. Depending on the switch that supports the ISDN line, the ISDN line could be assigned zero, one, or two SPIDs.

Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS ip helper-address functionality.

Time-Based Access Lists

It is now possible to implement access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name, and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

RIP Enhancements

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces.

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There were two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits from being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

ISDN MIB RFC2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. It controls all aspects of ISDN interfaces. RFC2127 provides information on the physical Basic Rate Interfaces (BRIs), control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 800 series.

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release—the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

Caveat CSCdr91706 and IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to `http://router-ip/anytext?/` is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

Cisco 800 Series Router Clock—CSCdp09409

To run IPsec successfully, the Cisco 800 series router clock needs to be set accurately. Cisco 800 series router clocks are set and maintained using Simple Network Time Protocol (SNTP). For best results, set up a Network Time Protocol (NTP) server to periodically send time information messages to Cisco 800 series routers. See the SNTP configuration and command reference documentation for configuration instructions. If you do not have an NTP server, you must reset the Cisco 800 series router clock using the `clock set` command each time you restart the router.

The SNTP configuration documentation is available in the chapter “Monitoring the Router and Network” in the “System Management” volume of the *Configuration Fundamentals Configuration Guide* in the Cisco IOS documentation set.

The SNTP command reference documentation is available in the chapter “Router and Network Monitoring Commands” in the “System Management Commands” volume of the *Configuration Fundamentals Command Reference* manual in the Cisco IOS documentation set.

Downloading Images

Before attempting to download new images, you must first delete files in your router’s Flash memory. Be sure to use the **delete** command, not **erase**, to free up space. Entering **erase** will remove all files, including the configuration.

Cisco IOS Release 12.0(4)XM

The images introduced in Release 12.0(4)XM apply to the Cisco 805 router *only*. They are not supported by the Cisco 801, 802, 803 or 804. For more information about this special release, see the *Release Notes for the Cisco 805 Router for Cisco IOS Release 12.0(4)XM* on CCO.

Dial Peer Limitation

The **isdn answer1** and **isdn answer2** commands determine which called telephone numbers, for example, 555-1111 and 555-2222, a Cisco 800 series router can answer. Using these commands limits a router to using the two dial peers that contain the telephone numbers 555-1111 and 555-2222. (When not using these commands, a router can use up to six dial peers.)

A sample scenario in which the **isdn answer1** and **isdn answer2** commands are used is when a Cisco 801 or Cisco 803 router is connected with other ISDN devices to an ISDN S-bus.

Excessive ISDN Line Activation

The following protocols send updates that can cause an ISDN line to be activated excessively thereby increasing your monthly ISDN line cost:

- IP
- User Datagram Protocol (UDP)
- IPX
- Cisco Discovery Protocol (CDP)
- Simple Network Time Protocol (SNTP)

For information on preventing this situation, refer to the *Cisco 800 Series Routers Software Configuration Guide*. This guide contains information on setting up extended access lists to prevent IP, UDP, IPX, and SNTP updates from activating the ISDN line. For CDP, make certain that you enter the **no cdp enable** command to disable CDP.

Hanging During Boot

If an illegal console configuration is issued to the router, the console will then fail the POST test during boot and cause the router to hang. There is no way to recover a unit in this state except for pulling the soldered boot flash and re-burning the boot ROM.

This problem has been resolved in TinyROM version 1.0(3), a downloadable ROM upgrade available from CCO. Please contact Cisco to upgrade to this version or later, and prevent this problem from occurring.

Phone Mate Answering Machine Model 9200

Phone Mate answering machine model 9200 failed to recognize the ringing signal sent by AMD R79 ringing SLIC. This was confirmed by testing against Phone Mate model 3750 and newer model 9300.

NVRAM Data Storage Limitation in Release 12.0(4)T and Earlier

The Cisco 800 router nonvolatile RAM (NVRAM) has a configuration data storage limitation in Cisco IOS Release 12.0(4)T and earlier releases. This problem was resolved in Release 12.0(5)T. Because of this limitation, you might not be able to save the digital certificate into the NVRAM if a large amount of other configuration data already exists. Cisco recommends that you not power off your router if you were not able to save the digital certificate. If you power off your router without successfully saving the digital certificate, you will need to generate the keys and request a new digital certificate from the Certificate Authority (CA) server after powering on the router again.

B Channel Activation

When a call comes in, a B channel is activated. If the amount of traffic on the B channel exceeds a threshold, the other B channel is activated. If the amount of traffic falls below the threshold, one of the B channels is deactivated. The B channel that is initially activated when the call comes in is not necessarily B1 nor is the B channel that is deactivated when the traffic level lessens necessarily B2.

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
- 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 7, *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 7. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 7, *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 24 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
- 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 7 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 7, 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 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.

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 7 specifies information about affected and repaired software versions.



Note All dates within this table are subject to change.

Table 7 *Affected and Repaired Software Versions*

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 ⁴	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S ⁵ , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.

Table 7 *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(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 in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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

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

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

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*, which lists severity 1 and 2 caveats and is located on CCO and the Documentation CD-ROM.



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at <http://www.cisco.com/support/bugtools>

Caveats for Release 12.0(7)T

This section describes possibly unexpected behavior by Release 12.0(7)T, specific to the Cisco 800 series routers. Only severity 1 and 2 caveats are included.

CSCdp09409

To run IPSec successfully, the Cisco 800 series router clock needs to be set accurately. Cisco 800 series router clocks are set and maintained using Simple Network Time Protocol (SNTP). For best results, set up a Network Time Protocol (NTP) server to periodically send time information messages to Cisco 800 series routers. See the SNTP configuration and command reference documentation for configuration instructions. If you do not have an NTP server, you must reset the Cisco 800 series router clock using the **clock set** command each time you restart the router.

The SNTP configuration documentation is available in the chapter “Monitoring the Router and Network” in the “System Management” volume of the *Configuration Fundamentals Configuration Guide* in the Cisco IOS documentation set.

The SNTP command reference documentation is available in the chapter “Router and Network Monitoring Commands” in the “System Management Commands” volume of the *Configuration Fundamentals Command Reference* manual in the Cisco IOS documentation set.

CSCdp20454

The command **show isdn status** does not show the correct **spid1/spid2** status. The command displays the SPIDs as not valid. This is only a cosmetic problem in Cisco IOS release 12.0(7)T; therefore, the SPIDs might actually be valid. To determine whether or not the SPIDs are valid, in Privileged EXEC mode use the command **isdn call int bri 0 phone_number** to make a call to the remote router. With the command **debug isdn q931** turned on, the SPIDs are valid if the call “setup” and “teardown” appear identical. Alternatively, make a call to the remote router by using the command **ping remote_IP_address**. Receiving a successful response indicates that the SPIDs are valid. An example of cosmetically incorrect command output is displayed as follows:

```
router# show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface
  dsl 0, interface ISDN Switchtype = basic-ni
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 123, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    TEI = 124, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    TEI 123, ces = 1, state = 8(established)
      spid1 configured, spid1 sent, spid1 NOT valid
    TEI 124, ces = 2, state = 8(established)
      spid2 configured, spid2 sent, spid2 NOT valid
  Layer 3 Status:
    0 Active Layer 3 Call(s)
  Activated dsl 0 CCBs = 0
  The Free Channel Mask: 0x80000003
  Total Allocated ISDN CCBs = 0
```

CSCdp60086

The **frame-relay tunnel** subcommand is not available on the Cisco 1600, 1700, and 800 series platforms. This subcommand is only available in IOS images corresponding to Enterprise feature sets:

```
router(config-if)# frame-relay route 19 interface ?
      Serial Serial
      Tunnel Tunnel interface
```

CSCdp62196

If a Cisco 804 router is running the Cisco IOS Release 12.0(4)T1 IP image and using an electrical phone plugged into a plain old telephone service (POTS) port with the ISDN line provisioned with US Caller ID, the router might have intermittent ringing problems.

This caveat has been resolved in Cisco IOS Release 12.1(3)T.

Related Documentation

The following sections describe the documentation available for the Cisco 800 series. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

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

Use these release notes with these documents:

- Release-Specific Documents, page 29
- Platform-Specific Documents, page 30
- Feature Modules, page 31
- Cisco IOS Software Documentation Set, page 31

Release-Specific Documents

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

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

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

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

Service & Support: Technical Documents

- *Caveats for Cisco IOS Release 12.0 T*

This document contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats

On the Documentation CD-ROM at:

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



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at <http://www.cisco.com/support/bugtools>

Platform-Specific Documents

These documents are available for the Cisco 800 series on CCO and the Documentation CD-ROM:

- *Cisco 800 Series Router Quick Start Guide*
- *Quick Start Guide - Setting Up the Cisco 805 Router*
- *Cisco 800 Series Routers Hardware Installation Guide*
- *Cisco 805 Router Hardware Installation Guide*
- *Cisco 800 Series Routers Software Configuration Guide*
- *Cisco 805 Router Software Configuration Guide*
- Release Notes for Cisco 800 Series Routers
- Release Notes for the Cisco 805 Router
- *Configuring Cisco IOS Software Features*
- *Cisco 800 Fast Step Quick Start Guide*
- *Cisco Fast Step documentation for the 800 series routes*
- *Regulatory Compliance and Safety Information*
- *Regulatory Compliance and Safety Info for Cisco 805 Router*
- *Upgrading Memory in the Cisco 800 Series Routers*

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Fixed Access Routers: Cisco 801–804 Routers or Cisco 805 Router

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Fixed Access Routers: Cisco 801–804 Routers or 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.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

On the Documentation CD-ROM at:

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

On the Documentation CD-ROM at:

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

Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.



Note

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

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

Table 8 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <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> 	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> 	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> 	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> 	



Note

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

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.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 is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered Cisco.com users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed documents, or by sending mail to Cisco.

Cisco.com

Cisco continues to revolutionize how business is done on the Internet. Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through Cisco.com, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access Cisco.com in the following ways:

- WWW: www.cisco.com
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using Cisco.com to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a Cisco.com log-in account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/public/technotes/tech_sw.html

This URL is subject to change without notice. If it changes, point your Web browser to Cisco.com, press **Login**, and click on this path: **Technical Assistance Center: Technical Tips**.

The following sections are provided from the Technical Tips page:

- **Access Dial Cookbook**—Contains common configurations or recipes for configuring various access routes and dial technologies.
- **Field Notices**—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- **Frequently Asked Questions**—Describes the most frequently asked technical questions about Cisco hardware and software.
- **Hardware**—Provides technical tips related to specific hardware platforms.
- **Hot Tips**—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- **Internetworking Features**—Lists tips on using Cisco IOS software features and services.
- **Sample Configurations**—Provides actual configuration examples that are complete with topology and annotations.

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 29.

AtmDirector, Browse with Me, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, IOS, IP/TV, LightStream, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or 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. (0011R)

Copyright © 1999–2000, Cisco Systems, Inc.
All rights reserved.

