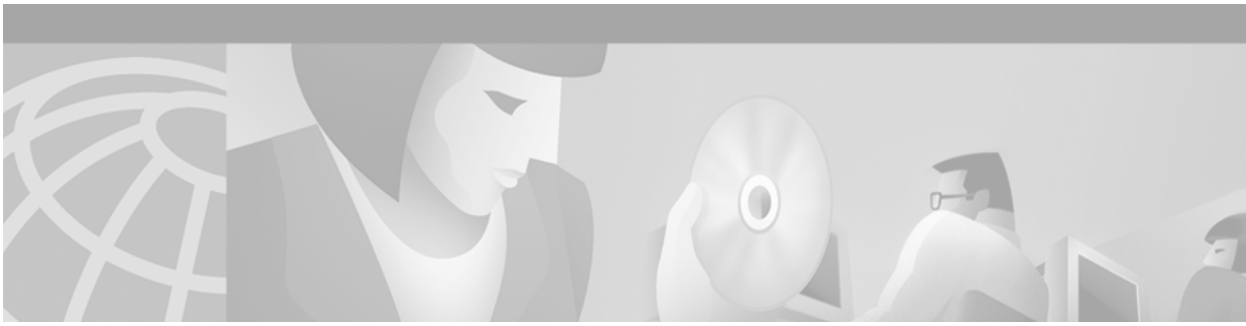

Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XT

March 18, 2002

Cisco IOS Release 12.2(2) XT3

OL-1868-02 Rev. B0

These release notes describe new features and significant software components for the Cisco 1700 series routers that support Cisco IOS Release 12.2 T, up to and including Release 12.2(2)XT. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on CCO and the Documentation CD-ROM.

For a list of the software caveats that apply to Release 12.2(2)XT, refer to the section "Caveats" and to the online *Caveats for Cisco IOS Release 12.2 T* document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

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

System Requirements

This section describes the system requirements for Release 12.2(2)XT and includes the following sections:

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(2)XT on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1750 and 1751 Routers	Cisco 1700 IOS IP/ ADSL/VOX Plus	IP/ADSL/VOX Plus	c1700-sv8y7-mz	16 MB	48 MB	RAM
Cisco 1751 Router	Cisco 1700 IOS IP/ ADSL/VOX/FW/IDS Plus	IP/ADSL/VOX/ FW/ IDS Plus	c1700-o3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/VOX Plus IPSec 3DES	IP/ADSL/VOX Plus IPSec 3DES	c1700-k9sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/VOX/FW/IDS Plus IPSec 3DES	IP/ADSL/VOX/ FW/ IDS Plus IPSec 3DES	c1700-k9o3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/VOX Plus IPSec 56	IP/ADSL/VOX Plus IPSec 56	c1700-k8sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/VOX/FW/IDS Plus IPSec 56	IP/ADSL/VOX/ FW/ IDS Plus IPSec 56	c1700-k8o3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/ VOX/FW/IDS Plus IPSec 3DES	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 3DES	c1700-bk9no3r2sv8y7-mz	32 MB	64 MB	RAM
	Cisco 1700 IOS IP/ ADSL/IPX/AT/IBM/ VOX/FW/IDS Plus IPSec 56	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 56	c1700-bk8no3r2sv8y7-mz	32 MB	64 MB	RAM

Hardware Supported

Cisco IOS Release 12.2(2)XT supports the following Cisco 1700 series routers:

- Cisco 1750, 1750-2V, and 1750-4V routers
- Cisco 1751 and 1751-V routers

The Cisco 1750, 1750-2V, and 1750-4V routers run data and data-and-voice images, providing analog voice support. Cisco 1751 and 1751-V routers run data and data-and-voice images, providing digital and analog voice support.

For detailed descriptions of the new hardware features, see the documents listed in the "Platform-Specific Documents" section on page 25.

Cisco 1750, 1750-2V, and 1750-4V Routers

The voice-and-data capable Cisco 1750, 1750-2V and 1750-4V routers provide global Internet and company intranet access and includes the following:

- Voice-over-IP (VoIP) voice-and-data functionality; the router can carry voice traffic (for example, telephone calls and faxes) over an IP network.
- Support for virtual private networking.
- Modular architecture.
- Network device integration.

The Cisco 1750, 1750-2V and 1750-4V routers have the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with manual override available).
- One voice interface card (VIC) slot—Supports a single voice interface card with two ports per card.
- Two WAN interface card (WIC) slots for either WICs or VICs.
- Synchronous serial interfaces on serial WICs.
- Asynchronous serial interfaces on serial WICs.
- ISDN WICs—ISDN dialup and ISDN leased line (IDSL) at 144 kbps; encapsulation over ISDN leased line; Frame Relay and PPP.
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial).
- One console port.
- One internal expansion slot—Supports hardware-assisted services such as encryption (up to T1/E1 speeds).
- RISC Processor—Motorola MPC860T PowerQUICC at 48 MHz.
- One security slot that supports Kensington or similar lockdown equipment.
- DRAM: 16 MB default, expandable to 48 MB.
- Flash memory: 4 MB default, expandable to 16 MB.
- Desktop form factor.

The Cisco 1750, 1750-2V and 1750-4V routers support any combination of one or two of the following WICs:

- WIC-1T—One-port high speed serial (sync/async)(T1/E1).
- WIC-2T—Two-port high speed serial (sync/async) (T1/E1).
- WIC-2A/S—Two-port low speed serial (sync/async) (up to 128 kbps).
- WIC-1B-S/T—One-port ISDN BRI S/T.
- WIC-1B-U—One-port ISDN BRI U with integrated NT1.
- WIC-1DSU-56K4—One-port integrated 56/64 kbps 4-wire DSU/CSU.
- WIC-1DSU-T1—One-port integrated T1 / Fractional T1 DSU/CSU.
- WIC-1ADSL—One-port asymmetric digital subscriber line.
- WIC-1ENET—One-port 10Base-T Ethernet interface.

The Cisco 1750, 1750-2V and 1750-4V routers support any combination of one or two of the following voice interface cards:

- VIC-2FXS—Two-port Foreign Exchange Station (FXS) voice interface card.
- VIC-2FXO—Two-port Foreign Exchange Office (FXO) voice interface card.
- VIC-2FXO-EU—Two-port FXO voice interface card for Europe.
- VIC-2E/M—Two-port Ear and Mouth (E & M) voice interface card.
- VIC-2FXO-M1—Two-port FXO for the United States with battery reversal.
- VIC-2FXO-M2—Two-port FXO for Europe with battery reversal.
- VIC-2FXO-M3—Two-port FXO for Australia.

Cisco 1751 and 1751-V Routers

The voice-and-data capable Cisco 1751 and 1751-V routers provide global Internet and company intranet access and include the following:

- Voice-over-IP (VoIP) voice-and-data functionality; the router can provide support for digital and analog voice traffic (for example, telephone calls and faxes) over an IP network.
- Support for virtual private networking.
- Modular architecture.
- Network device integration.

The Cisco 1751 and 1751-V routers have the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with manual override available).
- IEEE 802.1Q VLAN support.
- One VIC slot—Supports a single voice interface card with two ports per card.
- Two WIC slots for either WICs or VICs.
- Synchronous serial interfaces on serial WICs.
- Asynchronous serial interfaces on serial WICs.
- ISDN WICs—ISDN dialup and ISDN leased line (IDSL) at 144 kbps; encapsulation over ISDN leased line; Frame Relay and PPP.

- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial).
- One console port.
- One internal expansion slot—Supports hardware-assisted services such as encryption (up to T1/E1 speeds).
- RISC Processor—Motorola MPC860P PowerQUICC at 48.384 MHz.
- One security slot that supports Kensington or similar lockdown equipment.
- DRAM:
  - Cisco 1751: 32 MB default, expandable to 96 MB.
  - Cisco 1751-V: 64 MB default, expandable to 128 MB.
- Flash memory:
  - Cisco 1751: 16 MB.
  - Cisco 1751-V: 32 MB.
- Desktop form factor.

The Cisco 1751 and 1751-V routers support any combination of one or two of the following WICs:

- WIC-1T—One-port high speed serial (sync/async)(T1/E1).
- WIC-2T—Two-port high speed serial (sync/async) (T1/E1).
- WIC-2A/S—Two-port low speed serial (sync/async) (up to 128 kbps).
- WIC-1B-S/T—One-port ISDN BRI S/T.
- WIC-1B-U—One-port ISDN BRI U with integrated NT1.
- WIC-1DSU-56K4—One-port integrated 56/64 kbps 4-wire DSU/CSU.
- WIC-1DSU-T1—One-port integrated T1 / Fractional T1 DSU/CSU.
- WIC-1ADSL—One-port asymmetric digital subscriber line.
- WIC-1ENET—One-port 10Base-T Ethernet interface.

The Cisco 1751 and 1751-V routers support any combination of one, two or three of the following VICs:

- VIC-2FXS—Two-port Foreign Exchange Station (FXS) voice interface card.
- VIC-2FXO—Two-port Foreign Exchange Office (FXO) voice interface card.
- VIC-2FXO-EU—Two-port FXO voice interface card for Europe.
- VIC-2E/M—Two-port Ear and Mouth (E&M) voice interface card.
- VIC-2FXO-M1—Two-port FXO for the United States with battery reversal.
- VIC-2FXO-M2—Two-port FXO for Europe with battery reversal.
- VIC-2FXO-M3—Two-port FXO for Australia.
- VIC-2BRI-NT/TE—Two-port ISDN interface.
- VIC-2DID—Two-port direct inward-dialing voice interface card.

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 1700 series router, log in to the 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) c1700 Software (c1700-sv8y7-mz), Release 12.2(2)XT, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Software Installation and Upgrade Procedures* located at: http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Sets

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 12.2(2)XT supports the same feature sets as Releases 12.2 and 12.2 T, but Release 12.2(2)XT includes new features supported by the Cisco 1700 series routers.

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 can be denied or subject to delay due to United States government regulations. When applicable, the 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.

Table 2 (Parts 1 and 2) lists the features and feature sets supported by the Cisco 1700 series routers in Cisco IOS Release 12.2(2)XT. The table uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.2(2)XT” means the feature was introduced in 12.2(2)XT. If a cell in this column is empty, the feature was included in the initial base release.

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. Additional features are listed in the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set for the Cisco 1700 Series Routers, Part 1 of 2

Features	In	Feature Sets			
		IP/ADSL/VOX Plus	IP/ADSL/VOX/ FW/ IDS Plus	IP/ADSL/VOX Plus IPSec 3DES	IP/ADSL/VOX/ FW/ IDS Plus IPSec 3DES
IP Class of Service Mapping to ATM Quality of Service					
Committed Access Rate	12.2(2)XQ	Yes	Yes	Yes	Yes
Differentiated Services (class based marking)	12.2(2)XQ	Yes	Yes	Yes	Yes
Low Latency Queuing (LLQ, also called PQ/CBWFQ)	12.2(2)XQ	Yes	Yes	Yes	Yes
Multilink PPP with Link Fragmentation and Interleaving over ATM	12.2(2)XQ	Yes	Yes	Yes	Yes
Weighted Random Early Detection	12.2(2)XQ	Yes	Yes	Yes	Yes
IP Multicast					
Bidirectional PIM	12.2(2)XH	Yes	Yes	Yes	Yes
IP Routing Protocols					
OSPF flooding reduction	12.2(2)XH	Yes	Yes	Yes	Yes
LAN					
Support of Two WIC-1ENET adapters	12.2(2)XJ	No	No	No	No
Multimedia and Quality of Service					
H.323 V2 enhancements	12.2(2)XH	No	No	No	No
Quality-of-service voice enhancements	12.2(2)XH	No	No	No	No
H.323 version 2 phase 2 enhancements	12.2(2)XH	No	No	No	No
NBAR	12.2(2)XH	No	No	No	No
QDM	12.2(2)XH	No	No	No	No
Multiservice Applications —Voice					
Cisco IOS Telephony Service[1]	12.2(2)XT	Yes	Yes	Yes	Yes
Survivable Remote Site Telephony (SRST), Version 1[2]	12.2(2)XW	Yes	Yes	Yes	Yes
Survivable Remote Site Telephony (SRST), Version 2[3]	12.2(2)XT	Yes	Yes	Yes	Yes
Voice-over-Frame Relay (Cisco 175x only)	12.2(2)XH	Yes	Yes	Yes	Yes
Security					
Secure Shell version 1 integrated client	12.2(2)XH	No	No	Yes	Yes
SSH version 1 server support	12.2(2)XH	Yes	Yes	Yes	Yes
Virtual Private Network (VPN) Module for the Cisco 1700 series routers	12.2(2)XH	No	No	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 1700 Series Routers, Part 1 of 2 (continued)

Features	In	Feature Sets			
		IP/ADSL/VOX Plus	IP/ADSL/VOX/ FW/ IDS Plus	IP/ADSL/VOX Plus IPSec 3DES	IP/ADSL/VOX/ FW/ IDS Plus IPSec 3DES
Voice					
Caller ID on FXS, FXO-M1, and FXO-M2 VCI interfaces	12.2(2)XJ	Yes	Yes	Yes	Yes
Support for Two-Port analog DID VIC for Cisco 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes
Support for Two-Port FXO-M1 VIC for Cisco 1750 & 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes
Support for Two-Port FXO-M2 VIC for Cisco 1750 & 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes
WAN/Voice					
Frame Relay switching enhancements: shaping and policing	12.2(2)XH	Yes	Yes	Yes	Yes
Operations Administration Maintenance (OAM) Support for F5 Continuity Check (CC) Segment	12.2(2)XJ	Yes	Yes	Yes	Yes
Single-Port Ethernet WIC for Cisco 1700 Series Routers	12.2(2)XH	Yes	Yes	Yes	Yes
Two-port ISDN VIC for Cisco 1751 Routers	12.2(2)XH	Yes	Yes	Yes	Yes

1. In Cisco IOS Release 12.2(2)XT, the feature name “Cisco IP Keyswitch Version 2.0” changed to “Cisco IOS Telephony Service Version 2.0" and the command mode changed from “keyswitch-configuration mode” to “telephony-service configuration mode”.
2. SRST is supported on the Cisco 1750 router by the Release 12.2(2)XW image IP/VOX Plus only.
3. SRST is supported on the Cisco 1750 router by the image IP/ADSL/VOX Plus only.

Table 2 Feature List by Feature Set for the Cisco 1700 Series Routers, Part 2 of 2

Features	In	Feature Sets			
		IP/ADSL/VOX Plus IPSec 56	IP/ADSL/VOX/ FW/ IDS Plus IPSec 56	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 3DES	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 56
IP Class of Service Mapping to ATM Quality of Service					
Committed Access Rate	12.2(2)XQ	Yes	Yes	Yes	Yes
Differentiated Services (class based marking)	12.2(2)XQ	Yes	Yes	Yes	Yes
Low Latency Queuing (LLQ, also called PQ/CBWFQ)	12.2(2)XQ	Yes	Yes	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 1700 Series Routers, Part 2 of 2 (continued)

Features	In	Feature Sets			
		IP/ADSL/VOX Plus IPSec 56	IP/ADSL/VOX/ FW/ IDS Plus IPSec 56	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 3DES	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 56
Multilink PPP with Link Fragmentation and Interleaving over ATM	12.2(2)XQ	Yes	Yes	Yes	Yes
Weighted Random Early Detection	12.2(2)XQ	Yes	Yes	Yes	Yes
IP Multicast					
Bidirectional PIM	12.2(2)XH	Yes	Yes	Yes	Yes
IP Routing Protocols					
OSPF flooding reduction	12.2(2)XH	Yes	Yes	Yes	Yes
LAN					
Support of Two WIC-1ENET adapters	12.2(2)XJ	No	No	No	No
Multimedia and Quality of Service					
H.323 V2 enhancements	12.2(2)XH	No	No	No	No
Quality-of-service voice enhancements	12.2(2)XH	No	No	No	No
H.323 version 2 phase 2 enhancements	12.2(2)XH	No	No	No	No
NBAR	12.2(2)XH	No	No	No	No
QDM	12.2(2)XH	No	No	No	No
Multiservice Applications —Voice					
Cisco IOS Telephony Service[1]	12.2(2)XT	Yes	Yes	Yes	Yes
Survivable Remote Site Telephony (SRST), Version 1[2]	12.2(2)XW	Yes	Yes	Yes	Yes
Survivable Remote Site Telephony (SRST), Version 2[3]	12.2(2)XT	Yes	Yes	Yes	Yes
Voice-over-Frame Relay (Cisco 175x only)	12.2(2)XH	Yes	Yes	Yes	Yes
Security					
Secure Shell version 1 integrated client	12.2(2)XH	Yes	Yes	Yes	Yes
SSH version 1 server support	12.2(2)XH	Yes	Yes	Yes	Yes
Virtual Private Network (VPN) Module for the Cisco 1700 series routers	12.2(2)XH	Yes	Yes	Yes	Yes
Voice					
Caller ID on FXS, FXO-M1, and FXO-M2 VCI interfaces	12.2(2)XJ	Yes	Yes	Yes	Yes
Support for Two-Port analog DID VIC for Cisco 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 1700 Series Routers, Part 2 of 2 (continued)

Features	In	Feature Sets			
		IP/ADSL/VOX Plus IPSec 56	IP/ADSL/VOX/ FW/ IDS Plus IPSec 56	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 3DES	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS Plus IPSec 56
Support for Two-Port FXO-M1 VIC for Cisco 1750 & 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes
Support for Two-Port FXO-M2 VIC for Cisco 1750 & 1751 Routers	12.2(2)XJ	Yes	Yes	Yes	Yes
WAN/Voice					
Frame Relay switching enhancements: shaping and policing	12.2(2)XH	Yes	Yes	Yes	Yes
Operations Administration Maintenance (OAM) Support for F5 Continuity Check (CC) Segment	12.2(2)XJ	Yes	Yes	Yes	Yes
Single-Port Ethernet WIC for Cisco 1700 Series Routers	12.2(2)XH	Yes	Yes	Yes	Yes
Two-port ISDN VIC for Cisco 1751 Routers	12.2(2)XH	Yes	Yes	Yes	Yes

1. In Cisco IOS Release 12.2(2)XT, the feature name “Cisco IP Keyswitch Version 2.0” changed to “Cisco IOS Telephony Service Version 2.0" and the command mode changed from “keyswitch-configuration mode” to “telephony-service configuration mode”.
2. SRST is supported on the Cisco 1750 router by the Release 12.2(2)XW image IP/VOX Plus only.
3. SRST is supported on the Cisco 1750 router by the image IP/ADSL/VOX Plus only.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1700 series for Release 12.2(2)XT.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT3

No new hardware and software features are supported by the Cisco 1700 series for Cisco IOS Release 12.2(2) XT3.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT2

No new hardware and software features are supported by the Cisco 1700 series for Cisco IOS Release 12.2(2) XT2.

New Hardware and Software Features in Cisco IOS Release 12.2(2) XT1

No new hardware and software features are supported by the Cisco 1700 series for Cisco IOS Release 12.2(2) XT1.

New Software Features in Cisco IOS Release 12.2(2)XT

The following section describes the new software features supported by the Cisco 1700 series for Release 12.2(2)XT:

Cisco IOS Telephony Service

The Cisco IOS Telephony Service feature, a part of IP Telephony Services, provides basic Cisco IP phone call-handling capabilities in a LAN environment on the Cisco routers. This feature enables the Cisco multiservice routers to provide Cisco IOS Telephony Service for the Cisco IP Phone 7960, Cisco IP Phone 7940, Cisco IP Phone 7910, and Cisco IP Conference Station 7935. Cisco IOS Telephony Service also helps download phone software images and configures and manages the Cisco IP phones in a LAN, to accommodate the telephony system of a small office with a small number of extensions.

Note You need to purchase a feature license to turn this new feature on. You also need an account on Cisco.com to access the Cisco IP phone firmware versions.

For more information, see the document *Cisco IOS Telephony Service*:
http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/index.htm

Survivable Remote Site Telephony—Version 2.0

The Survivable Remote Site Telephony (SRST) Version 2.0 feature provides the Cisco CallManager application with fallback support for Cisco IP phones attached to local Ethernet router interfaces. Prior to SRST, if WAN connectivity was lost between a remote branch office router and a remote primary,

secondary, or tertiary Cisco CallManager, Cisco IP phones at the branch office were unusable for the duration of the failure. Using SRST, Cisco 1750 and 1751 series routers provide call-handling support for up to 24 Cisco IP phones and 48 lines when the WAN connection is down or connectivity to the Cisco CallManager is lost.

Cisco CallManager 3.0 with SRST automatically detects any failures between Cisco IP phones at remote sites and Cisco branch office multi-service routers, attached across a WAN. If a failure occurs, the SRST feature uses Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch router and provide call-processing service for the Cisco IP phones. During a failure, the Cisco IP phone displays a message indicating the Cisco IP phone is in the Cisco CallManager fallback mode and able to perform a limited set of functions. When WAN connectivity is restored, call-handling support for Cisco IP phones returns to the primary Cisco CallManager.

Note You need to purchase a feature license to turn this new feature on. You also need an account on Cisco.com to access the Cisco IP phone firmware versions.

The SRST feature supports up to six lines per phone, 24 phones, and 48 lines per system, with the following capabilities:

- Redundant Call Processing if a WAN failure occurs:
  - Re-homing of IP phones to a local router
  - Local Extension-to-Extension calls
  - Extension-to-PSTN calls
  - No service disruption when the WAN link is restored
- Calling Services during a WAN Failure:
  - Speed dial and last-number redial
  - Direct Outward Dial (DOD) calling
  - Direct Inward Dial (DID) calling
  - Caller ID and Automatic Number Identification (ANI) support
  - Calling Party Name
  - Distinctive Ringing
  - Transfer (without consultation)
  - Call hold and pickup
  - Call park and retrieve
  - Call waiting
- Centralized configuration and management
- Access at every remote site to all Cisco CallManager features during normal operations
- Remote maintenance and troubleshooting

For more information, see the document *Survivable Remote Site Telephony Version 2.0*: http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/fallbak2.htm

Limitations and Restrictions

The following sections contain Limitations and Restrictions for Cisco IOS Release 12.2(2)XT that can apply to the Cisco 1700 series. (Also, see the"Important Notes" section on page 14 and the "Caveats" section on page 15.)

Hardware Equipment and Software Features Not Supported

Release 12.2(2)XT does not support the following hardware equipment or software features, which are supported by some other Cisco IOS software releases on Cisco 1700 series routers:

- Cisco 1760 router
- G-standard Symmetrical High bit-rate Digital Subscriber Loop (G.SHDSL) WAN interface card
- Multiple 10Baset-T Ethernet WIC cards
- Locations for WIC-1ENET Single Port Ethernet WICs other than Slot 0
- Quality of Service (QoS) features on an ADSL link
- Cisco Hoot and Holler over IP feature

Note The Hoot and Holler network is a multi-point, four-wire audio-conference network that is always up so that communication is enabled with the push of a button when needed.

Cisco IOS HTTP Vulnerability—Caveat CSCdr91706

A defect in multiple releases of Cisco IOS software causes a Cisco router or switch to halt and reload if the Cisco IOS HTTP service is enabled, you attempt to browse to http://router-ip/anytext?/, and you supply the enable password when prompted. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco caveat CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This vulnerability can only be exploited if the enable password is known or not set. This caveat is not the same defect as caveat CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected Cisco IOS releases. Cisco urges all customers to upgrade to releases that are not vulnerable to this defect.

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

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(2)XT that can apply to the Cisco 1700 series. (Also, see the "Limitations and Restrictions" section on page 13 and the "Caveats" section on page 15.)

IP Phone Quantity with 10BaseT Interfaces

When data and voice are running on a Cisco router with a 10BaseT interface, the 10 Mbps bandwidth of the interface might negatively impact voice traffic. In this case, Cisco recommends connecting a maximum of 12 IP phones to the router, to keep the 10BaseT connection from becoming a bottleneck. For interfaces of 100 Mbps or higher, up to 24 IP phones are supported.

Fan Operation in Cisco 1700 Series Routers

The fans in some Cisco 1700 series routers stay off until thermally activated. The fans in Cisco 1760 and 1760-V routers are always on.

Flash defaults to Flash:1 on Multipartition Flash

When using a multipartition flash card, the various flash partitions are referred to as "flash:1:", "flash:2:", etc. If you specify only "flash" in a multipartition flash, the parser assumes "flash:1:." For example, if you enter **show flash all** the parser defaults to "show flash:1: all" and only the flash information for the first partition displays. To see information for all flash partitions, enter the command **show flash ?**. After all of the valid partitions are displayed, enter the command **show flash:xx: all** on each valid partition.

Peak Cell Rate and Sustainable Cell Rate Values

On Cisco 1700 routers, specify the Peak Cell Rate (PCR) and Sustainable Cell Rate (SCR) as multiples of 32 Kbps. Other rates are treated as the next lower value of a multiple of 32. For example, an entered PCR value of 150 is considered 128.

Using the boot flash Command

Booting a Cisco 1700 series router with the commands **boot flash** or **boot system flash** results in unpredictable behavior. To work around this problem, be sure to enter a colon (:) following both commands (for example, **boot flash:** or **boot system flash:.**)

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, and severity 3 caveats are the least serious of these three severity levels.

All caveats in Release 12.2 T are also in Release 12.2(2)XT. For information on caveats in Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document. For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. 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 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**: **BUG TOOLKIT**: **Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools/bugtool.shtml.

Open Caveats—Cisco IOS Release12.2(2) XT3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2) XT3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx04374

  If CLNS is configured on the SVI interface (Vlan), the SNPA/MAC is not learned correctly by the router in which the SVI is present. This results in the router sending packets to a non-existent destination MAC address.

  There is no workaround.

- CSCdw46537

  Symptom:

  SPAN doesn’t work after moving one port from multi span src ports. Disabling a source interface from a monitor session results in disabling the entire monitor session, not just the specified port.

  Workaround:

  If a particular source port is required to be removed form a SPAN session, stop the entire SPAN session and re-configure with only the required source ports.

- CSCdw29549

  Symptom:

  Port security failed when configuring secure MAC addresses on an irrelevant port. When Port Security is configured on two interfaces P1 & P2, and secure MAC addresses M1 & M2are configured on interfaces P1 & P2 respectively, P1 should only allow packets with source MAC address M1 and P2 should only allow M2. But if a packet with secure MAC address M1 ingresses port P1, then the switch treats it like a station movement and allows the packet to be switched.

  Workaround:

  Cisco Systems recommends that when station movement takes place, the MAC addresses associated with the port should be cleared in the switch's tables before moving them to another port.

- CSCdw14813

  Symptom:

  The command **show mac count** shows the wrong number of MAC addresses when compared to the count of addresses shown by the **show mac** command.

  There is no workaround.

- CSCdw20431

  Symptom:

  Traceback is seen on configuring the duplex and speed.

  There is no workaround.

Resolved Caveats—Cisco IOS Release12.2(2) XT3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2) XT3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv24152

  Symptom:

  A Cisco router that is running Cisco IOS Release 12.0(17)S and later 12.0 S releases may reset if Frame Relay has been incorrectly configured. If you apply the same data link control (DLC) value on an interface and on its subinterface twice in a row, the router may reset.

  There is no workaround.

- CSCdw14262

  Symptom:

  Cisco Voice over IP (VoIP) gateways that are running a Cisco IOS Release 12.2(1a) IP plus image may experience a high central processing unit (CPU) memory utilization condition at the CCH323_CT process.

  There is no workaround.

- CSCin02687

  Symptom:

  When using the Cisco 7200 series router as a Survivable Remote Site Telephony (SRST) and IOS telephony service router and making more than 30 three-party conference calls, the router crashes. The tracebacks point to the fast-ethernet interface that is being used to connect the router to the IP phones or rather the IP phone simulator.

  Workaround:

  Restrict the number of three-party conference calls.

- CSCdv62649

  Symptom:

  The command **ip tacacs source-interface** does not work properly.

  Workaround:

  If configured to use loopback interface for tacacs packets, the router may still use the interface address.

- CSCdw08182

  Symptom:

  The VWIC installed in NM-1FE2W appears in **show diag** response but not in the configuration.

  The router is recognizing that it has a VWIC-1MFT-T1 in a NM-1FE2W in the show diag. The problem is that the T1 controller doesn't appear in the configuration. The FastEthernet is present.

  There is no work-around.

- CSCdw26331

  Symptom:

  A call to a busy FXS port produces an incorrect release cause code. Calls may receive a "no route to destination" message and an incorrect clearing cause code (instead of a user busy cause code) when calls are placed to a Foreign Exchange Station (FXS) on a busy interface. Depending on the equipment that is used, the caller may receive a "number unobtainable" message or fast busy tones instead of a busy tone when this condition occurs.

  Workaround:

  Add a huntstop on the dial peer that is assigned to the FXS interface.

- CSCdw38767

  Symptom:

  Some ports on the NM-16ESW / NMD-36-ESW may not be assigned MAC addresses properly.

  Conditions:

  This occurs when the last digit of the base MAC address burnt in the NM cookie is in the range 0xF0-0xFF for NM-16ESW and range 0xDA-0xFF for NMD-36-ESW.

  Workaround:

  None.

- CSCdw46803

  Symptom:

  After a Cisco 1751 router that is running Cisco IOS Release 12.2(2)XT and that has a BRI network termination/traffic engineering (NT/TE) is reloaded, Layers 1 and 2 may become deactivated.

  Workaround:

  Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the BRI interface.

- CSCdw51152

  Symptom:

  PCI Fatal Error on DMA CH1

  When access to Flash/NVRAM occurs as a result of **write memory** or **show run** commands, and the CPU utilization is high due to heavy packet traffic, this error message can sometimes occur.

  This is due to the PCI device timing out on the PCI bus waiting for DMA access to memory.

  Workaround:

- CSCdu53333

  Symptom:

  A Cisco router that is running Cisco IOS Release 12.2(1) or 12.2(0.5g) may experience digital signal processor (DSP) reloads or fail to respond after the following DSP Timeout error messages are displayed:

  > %VTSP-3-DSP_TIMEOUT: DSP timeout on event 6: DSP ID=0x1: DSP error stats, chnl info(5, 13, 0) %VTSP-3-MSGSNDFAIL: channel:5/0:15 (54516) DSP ID:0x1 Message ID:0x47

  The problem is intermittant, and DSPs may hang indefinitely as rarely as only once every few weeks. The problem is likely to appear when T.38 fax mode is used and is likely to appear when "codec complexity medium" is configured for the voice card and there is frequent switching between the fax and voice modes.

  Workaround:

  This DSP firmware defect is fixed in DSP Release 3.6.15 / VCWare Release 9.19 and DSP Release 3.4.49 / VCWare Release 7.38, as well as newer versions of these firmware releases.

- CSCdw54986

  Symptom:

  A router with primary-ni switchtype will not be able to interoperate with switches that sends CLID/CLIP/CLIR information in FACILITY messages. The router does not accept the FACILITY and disconnects the call.

  Workaround:

  None

- CSCdw57198

  Symptom:

  SRST router with FXO ports typically has a connection plar (opx) to route an incoming call on the port to an extension in the router. With this problem, the incoming call cannot be transferred.

  There is no workaround.

- CSCdw62829

  Symptom:

  The High-Density Analog Voice/Fax Network Modules (NM-HDA) for the Cisco 2600 series and Cisco 3600 series routers support Local Voice Busyout (LVBO) features. The **busyout monitor** command can be configured under NM-HDA voice-ports to permit busyout monitoring of local interfaces or remote IP interfaces via Service Assurance Agent (SAA) probes. These features can be configured and can be saved to Non-Volatile RAM (NVRAM) successfully, but on a router reload, the boot-time parser rejects the **busyout monitor** commands.

  Any **busyout monitor** command configured under a voice-port on a NM-HDA will disappear from the running-configuration if the router is rebooted. This problem does not occur on VIC-2E/M, VIC-2FXS, and VIC-2FXO voice-ports housed on the NM-1V and NM-2V products.

  Workaround:

  Issue a **copy startup-config running-config** to re-assert the missing commands.

- CSCdw70410

  Symptom:

  A Cisco router may reload after a high-density analog voice or fax network module (NM-HDA) that is installed in a slot is replaced by another NM-HDA that has a different hardware configuration.

  Workaround:

  Use a replacement card that is the same as the original card. This condition will not occur if a card that is the same as the original is used or if a differently configured card is placed in a different slot.

- CSCdw71436

  Symptom:

  Under rare circumstances, a Cisco router may reload because of a segmentation violation (SegV) when fax calls are present.

  There is no workaround.

- CSCdw73302

  Symptom:

  When using a TCL IVR 2.0 application on a Cisco voice gateway for 2-stage calls, the configured translation rule may be applied for each received digit, instead of only for the initial digit.

  Workaround:

  None

- CSCdw73507

  Symptom:

  Ringback is not available for calls coming in from a PSTN. IP phones do not ringback on the network side. When a call comes in from a PSTN, the call should tell the PSTN end so that it can generate ringback on behalf of the IP phones by sending progress ind as 3.

  Workaround:

  None

- CSCdw75065

  Symptom:

  Alignment traceback when transfer and conference call. Tracebacks are observed during conference and at times, during regular calls. The tracebacks are on misaligned accesses to memory.

  Workaround:

  They are subsequently corrected by the hardware but prints to console are annoying and can be viewed as serious potential issues.

- CSCdw82677

  Symptom:

  Bad voice-quality during conference call. This happens when a Survivable Remote Site Telephony (SRST) ITS GW with loop-back-dns is used in conferencing with a remote GW and where a mis-match of codec types results if the GWs do not have the same codec type configured. Conferencing a-law and u-law mixes doesn't work as some legs in ITS end up with a-law and some with u-law which gives bad voice quality.

  Workaround:

  This fix is only applicable for a network that has a mixture of A-law and U-law codecs configured in the network. Configure all gateways in the network to use same codec type of either A-law or U-law.

- CSCdw84594

  Symptom:

  Show diag for Cisco 2600 series routers gives wrong values for NMs which uses TLV_IDPROM. This problem is only on Cisco 2600 series platform

  Conditions:

  While issuing **sh diag <slot>** command, HDA uses TLV_IDPROM. The hardware version, revision information, and other conditions are displayed wrongly.

  Workaround:

  None

- CSCdw85359

  Symptom:

  Caller ID is discarded when an incoming PSTN call through FXO-M1/FXS-M1 is transferred to another number. The Caller-ID displayed after the transfer is "From Private....".

  Workaround:

  None:

- CSCdx01445

  Symptom:

  The port does not go on-hook when a supervisory disconnect tone is sent from the PSTN. When call comes in through FXO port to IP Phone, the IP Phone goes into Alerting state. If the caller hangs up at this point, the PSTN sends a supervisory disconnect tone to the FXO where no action is taken which results in not freeing up the port immediately.

  Workaround:

  None

- CSCuk31298

  Symptom:

  The IP phone locks during a call to a call forward busy number. This condition occurs in a setup whereby the call forward busy feature is configured using the Cisco IOS Telephony Service (ITS) on an IP phone (phone A) to a second IP phone (phone B). When a call is made from phone A to another phone (phone C), the call can be answered normally.

  When a second call is placed from another phone to phone A via a loopback-directory number (loopback-dn), the call is forwarded to phone B. As this call is received, the original call is incorrectly cleared by the node on phone C while the call is still shown as “up” on phone A. When this condition occurs, phone A is no longer able to place or receive calls and has to be powered down to be restored to working condition.

  Workaround:

  This condition affects only the first IP phone in the internal control table on the router. The first IP phone is typically indicated as “ephone 1” when the **show ephone** EXEC command is issued.

  To prevent this condition from occurring when the router is operating in the ITS mode, add a dummy phone entry as the first IP phone or “ephone 1” in the internal control table on the router to prevent an active phone from being listed as the first IP phone in the internal control table of the router.

  Reload the router to ensure that the dummy phone occupies the first position in the control table. There is currently no workaround to this condition if the router is operating in the Survivable Remote Site Telephony (SRST) mode (call manager fall back).

- CSCuk31300

  Symptom:

  Ringing presented to caller before state of called number is known.

  When using loopback-dns for outgoing calls, the router presents a ringing tone to the IP phone caller as soon as the call has been routed and before the state of the called number is known.

  If the called number is busy, this can result in a ringing and then busy tone being played to the caller. This does not happen if loopback-dns are not used, or if they are used for incoming calls.

  Workaround.

  Do not use loopback-dns for outgoing calls.

- CSCuk31512

  Symptom:

  On a miss dialed call transfer, a new call shows previously dialed digits.

  When a Keyswitch IP phone user receives an incoming call, and they then attempt to transfer that call, but while dialling they realize they are dialling a wrong number, the transferrer has two options. If they incorrectly select "New Call", the phone displays the previous dialed digits. If the caller then dials more digits, these appear after the previous digits. The phone however only dials the digits presented after the "New Call" button was pressed, and the call is successful.

  Workaround.

  None

- CSCuk31658

  Symptom:

  On three-way calls setup by a Survivable Remote Site Telephony / Keyswitch IP phone, if the second call leg to be setup clears their call, the speech path from the IP phone where the conference was setup to the other phone is lost. The problem is observed only when the second call clears, and only if another IP phone is used in addition to the IP phone which set the conference up. Voice path is re-established if the phone that initiated the conference temporarily places the remaining caller on-hold and then immediately resumes the call.

  Workaround:

  None

- CSCdw62185

  This release integrates the DSPware 3.6.15 release. Upgrading to the DSPware 3.6.15 release to fix CSCdu53333 (dsp timeout) remedies the voice quality problem in this caveat.

Open Caveats—Cisco IOS Release12.2(2) XT2

There are no open caveats specific to Cisco IOS Release 12.2(2)XT2 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release12.2(2) XT2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XT2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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

Open Caveats—Cisco IOS Release12.2(2) XT1

There are no open caveats specific to Cisco IOS Release 12.2(2)XT2 that require documentation in the release notes.

- CSCdw19846

  The default application session IVR hunt does not work. When a default “application session” is configured under a POTS Dial Peer and a call is made from that port to another port, the call is dropped.

  There is no workaround.

Resolved Caveats—Cisco IOS Release12.2(2) XT1

There are no resolved caveats specific to Cisco IOS Release 12.2(2)XT3 that require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.2(2) XT

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2) XT and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr91706

  A defect in multiple releases of Cisco IOS software causes a Cisco router or switch to halt and reload if the Cisco IOS HTTP service is enabled, you attempt to browse to http://router-ip/anytext?/, and you supply the enable password when prompted. This defect can be exploited to produce a denial of service (DoS) attack. See the "Cisco IOS HTTP Vulnerability—Caveat CSCdr91706" section on page 13.

- CSCdw04503

  Call-forward commands not entered for E164 dial-peers.

  When dialplan pattern is configured for the local IP Phones, the existing call-forward commands under ephone-dn are not entered under the E.164 dial-peers created by the dialplan pattern command. This can cause a call not getting forwarded if you dial the entire E164 number.

  This problem happens only if you add or edit the existing dialplan pattern with call-forward commands already in place. One way to avoid this problem is to configure the right dialplan pattern before configuring the call-forward commands. Additionally, if you modify the dialplan pattern commands, configure the call forward commands again under ephone-dn. This creates the call-forward commands under the E164 dial-peers created.

- CSCdv78130

  Inconsistent music on hold (MOH) during conference.

  Music on hold works inconsistently in certain conditions. A calls B and conferences to C. B puts the conference on hold. Both A and C hear the MOH. B resumes the call and after a while puts the conference on hold again. Now only A (initiator) hears the MOH.

  There is no workaround.

- CSCdv72916

  Remote branch Analog Phone to IP Phone call disconnected during CM reconnect.

  Calls from Analog Phone to IP Phone during call-manager-fallback mode may get disconnected when the WAN link to CM comes back up. If a call is made in "normal mode" and the WAN link fails, the call stays up even though the WAN link failed. If the WAN link comes back up during the call and the call is between two IP phones or two analog phones, the call is not dropped. However, if the call is between an IP phone and an analog phone, the call is dropped.

  There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(2) XT

There are no resolved caveats specific to Cisco IOS Release 12.2(2) XT that require documentation in the release notes.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. 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 Cisco.com and the Documentation CD-ROM.

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

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(2)XT. They are located on Cisco.com and the Documentation CD-ROM (under the heading **Service & Support)**:

- To reach the *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XT*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco 1700 Series Routers**: **Cisco 1700 Series - Release Notes for Release 12.2(2)XT**

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T**

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  Technical Documents: **Product Bulletins**

- To reach the *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Caveats**

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

Platform-Specific Documents

Cisco 1750 Routers

These documents are available for the Cisco 1750 router on CCO and the Documentation CD-ROM at **Technical Documents**: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1750 Series Routers**:

- Installing Your Cisco 1700 Router Quick Start Guide
- Cisco 1750 Series Router Hardware Installation Guide
- Cisco 1700 Series Router Software Configuration Guide
- Cisco 1750 Series Router Release Notes
- Cisco 1750 Router Voice-over-IP quick start guide
- Cisco 1750 Voice-over-IP Software Configuration Guide
- Cisco 1700 Series (Cisco IOS) Router Release Notes
- Configuration Notes for Cisco 1700 Series Routers
- WAN Interface Cards Hardware Installation Guide

Cisco 1751 and 1751-V Routers

These documents are available for the Cisco 1751 and 1751-V routers on CCO and the Documentation CD-ROM at **Technical Documents**: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1751 Series Routers**:

- Installing Your Cisco 1700 Router Quick Start Guide
- Cisco 1751 Router Hardware Installation Guide
- Cisco 1751 Router Software Configuration Guide
- Cisco 1700 Series Router Software Configuration Guide
- Cisco 1751 Router Hardware Release Notes
- Configuring the Voice Interface Card for the Cisco 1751 Router
- Installing and Removing Packet Voice/fax DSP Modules
- Cisco 1700 Series (Cisco IOS) Router Release Notes
- Configuration Notes for Cisco 1700 Series Routers
- WAN Interface Cards Hardware Installation Guide

Feature Modules

Feature modules describe new features supported by Release 12.2 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 Release 12.2 feature modules, click this path (under the heading **Service & Support)**: **Technical Documents**: **Cisco IOS Software**: **Release 12.2**: **New Feature Documentation**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2X Releases**

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. 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. The Cisco IOS software documentation set is 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 one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. The Cisco IOS software documentation set is available on Cisco.com and on the Documentation CD-ROM (under the heading **Service & Support)** at:

Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Configuration Guides and Command References**

Release 12.2 Documentation Set

Table 3 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form (under the heading **Service & Support)** on Cisco.com and on the Documentation CD-ROM:

Technical Documents: **Cisco IOS Software**: **Release 12.2**

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

Table 3 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• Cisco IOS Configuration Fundamentals Configuration Guide • Cisco IOS Configuration Fundamentals Command Reference	Cisco IOS User Interfaces File Management System Management
• Cisco IOS Bridging and IBM Networking Configuration Guide • Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 • Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• Cisco IOS Dial Technologies Configuration Guide • Cisco IOS Dial Technologies Command Reference	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios

Table 3 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast	IP Addressing and Services IP Routing Protocols IP Multicast
• Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference	AppleTalk Novell IPX
• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• Cisco IOS Voice, Video, and Fax Configuration Guide • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• Cisco IOS Quality of Service Solutions Configuration Guide • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• Cisco IOS Security Configuration Guide • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• Cisco IOS Switching Services Configuration Guide • Cisco IOS Switching Services Command Reference	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 3 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• Cisco IOS Wide-Area Networking Configuration Guide • *Cisco IOS Wide-Area Networking Command Reference*	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference	General Packet Radio Service
• Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • *New Features in 12.2-Based Limited Lifetime Releases* • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

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 and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco products 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.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. 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 your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

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 provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, 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 can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Resolved Caveats—Cisco IOS Release 12.2(2) XT" section.