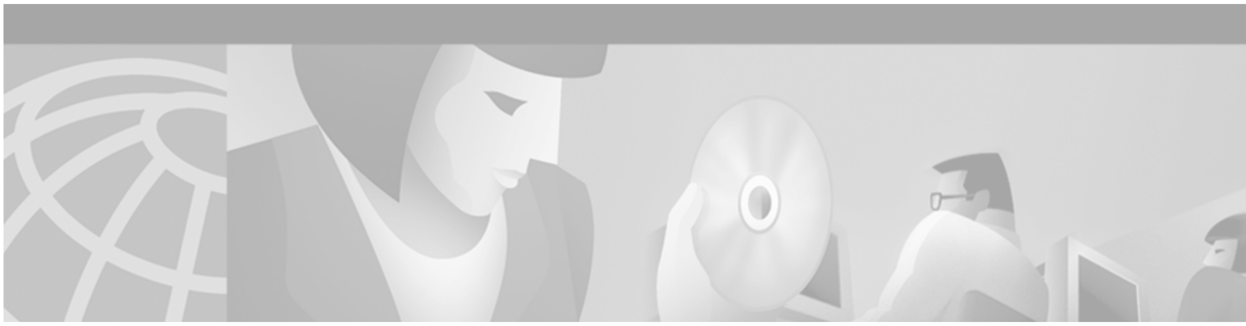

Release Notes for Cisco 1700 Series Routers for Cisco IOS Release 12.1 T

March 9, 2001

Note: You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hardcopy documents were printed.

These release notes for the Cisco 1700 series routers describe the enhancements provided in Cisco IOS Release 12.1 T. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T* that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.1* on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

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

Early Deployment Releases

These release notes describe the Cisco 1700 series routers for Cisco IOS Release 12.1 T, which is an early deployment (ED) release based on Cisco IOS Release 12.1. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

The following list shows the recent early deployment releases of the Cisco 1720 router:

- Release 12.0(1)XA
- Release 12.0(2)T to 12.0(7)T
- Release 12.1 T, up to 12.1(3)T

The following list shows the recent early deployment releases of the Cisco 1750 router:

- Release 12.0(5)XQ
- Release 12.0(7)T
- Release 12.1 T, up to 12.1(3)T

For more information, see the “Platform-Specific Documents” section on page 25 about accessing related release note documents.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1 T:

- Memory Requirements, page 3
- Hardware Supported, page 4
- Determining the Software Release, page 6
- Upgrading to a New Software Release, page 6
- Feature Set Tables, page 6

Memory Requirements

Table 1 Memory Requirements for the Cisco 1700 Series

Platforms	Feature Sets	Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1700 Series	IP Feature Sets	IP	c1700-y-mz	4 MB	20 MB	RAM
		IP Plus	c1700-sy-mz	8 MB	24 MB	RAM
		IP Plus IPSEC 56	c1700-sy56i-mz	8 MB	32 MB	RAM
		IP/FW/IDS	c1700-o3y-mz	4 MB	20 MB	RAM
		IP/FW/IDS Plus IPSec 56	c1700-o3sy56i-mz	8 MB	32 MB	RAM
		IP/IPX	c1700-ny-mz	4 MB	20 MB	RAM
		IP/IPX/FW/IDS Plus	c1700-no3sy-mz	8 MB	24 MB	RAM
		IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	24 MB	RAM
		IP/IPX/AT/IBM Plus	c1700-bnr2sy-mz	8 MB	32 MB	RAM
		IP/Voice Plus IPSEC 56	c1700-sv3y56i-mz	8 MB	48 MB[1]	RAM
		IP/Voice/FW/IDS Plus	c1700-o3sv3y-mz	8 MB	32 MB	RAM
		IP/Voice/FW/IDS Plus IPSec 56	c1700-o3sv3y56i-mz	8 MB	48 MB[1]	RAM
		IP/IPX/Voice/FW/IDS Plus	c1700-no3sv3y-mz	8 MB	32 MB	RAM
		IP Plus IPSEC 3DES	c1700-k2sy-mz	8 MB	32 MB	RAM
		IP/FW/IDS Plus IPSec 3DES	c1700-k2o3sy-mz	8 MB	32 MB	RAM
		IP/Voice Plus IPSEC 3DES	c1700-k2sv3y-mz	8 MB	32 MB	RAM
		IP/Voice/FW/IDS Plus IPSec 3DES	c1700-k2o3sv3y-mz	8 MB	48 MB[1]	RAM
		IP/IPX/ATM/IBM/Voice/FW/IDS Plus IPSEC 3DES	c1700-bk2no3r2sv3y-mz	20 MB	48 MB	RAM
		IP/IPX/ATM/IBM/FW/IDS Plus IPSec 3DES	c1700-bk2no3r2sy-mz	8 MB	48 MB[1]	RAM
		IP/IPX/AT/IBM/Voice/FW/IDS/Plus IPSec 56	c17000-bno3r2sv3y56i-mz	20 MB	48 MB	RAM
		IP/IPX/AT/IBM/FW/IDS Plus IPSec 56	c1700-bno3r2sy56i-mz	8 MB	48 MB[1]	RAM
		IP/Voice Plus	c1700-sv3y-mz	8 MB	32 MB	RAM

[1] 32 MB in Release 12.1(4)T and earlier releases.

Hardware Supported

Cisco IOS Release 12.1 T supports the Cisco 1700 series routers:

- Cisco 1720—Runs data images only.
- Cisco 1750—Runs data and data-plus-voice images.

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

Cisco 1720

The 1720 router provides Internet and intranet access and includes the following:

- Support for virtual private networking
- Modular architecture
- Network device integration

The Cisco 1720 router has the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with manual override available)
- Two WAN interface card slots
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial)
- One console port
- RISC Processor for high performance encryption
- One internal expansion slot for support of hardware-assisted services such as encryption (up to T1/E1) and compression
- DRAM memory: 16 MB default, expandable to 48 MB
- Flash memory: 4 MB default, expandable to 16 MB
- Desktop form factor

The Cisco 1720 router supports any combination of one or two of the following WAN interface cards, which are shared with the Cisco 1600, 2600, and 3600 routers:

- WIC-1T: One port high speed serial (sync/async)
- WIC-2T: Two port high speed serial (sync/async)
- 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
- WIC-1DSU-56K4: One port integrated 56/64 kbps 4-wire DSU/CSU
- WIC-1DSU-T1: One port integrated T1 / Fractional T1 DSU/CSU

Cisco 1750

The voice-and-data capable Cisco 1750 router provides 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 router has 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 slot—Supports a single voice interface card (Table 4) with two ports per card
- Two WAN interface card slots for either WAN interface cards (WICs) or voice interface cards (VICs)
- Synchronous serial interfaces on serial WAN interface cards
- Asynchronous serial interfaces on serial WAN interface cards
- ISDN WAN interface cards—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) and compression processor
- RISC Processor—Motorola MPC860T PowerQUICC at 48 MHz
- One security slot that supports Kensington or similar lockdown equipment
- DRAM memory: 16 MB default, expandable to 48 MB
- Flash memory: 4 MB default, expandable to 16 MB
- Desktop form factor
- Australian FXO-M3 (new in Release 12.1(5)T)

The Cisco 1750 router also supports any combination of one or two of the following WAN interface cards, which are shared with the Cisco 1600, 1720, 2600, and 3600 routers:

- 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

The Cisco 1750 router supports any combination of one or two of the following voice interface cards, which are shared with the Cisco 2600 and 3600 routers:

- VIC-2FXS: Two port Foreign Exchange Station (FXS) voice/fax interface card for voice/fax network module
- VIC-2FXO: Two port Foreign Exchange Office (FXO) voice/fax interface card for voice/fax network module
- VIC-2FXO-EU: Two port FXO voice/fax interface card for Europe
- VIC-2E/M: Two port Ear & Mouth (E&M) voice/fax interface card for voice/fax network module

Determining the Software Release

To determine the version of Cisco IOS software running on your Cisco 1700 series router, log in to the router and enter the **show version** EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 T Software (C1700-oy-mz), Version 12.1(5)T, 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 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.

Cisco IOS Release 12.1 T supports the same feature sets as Cisco IOS Release 12.1, but Release 12.1 T can include 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 may 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, Table 3, and Table 4 list the features and feature sets supported by the Cisco 1700 series in Cisco IOS Release 12.1 T. 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.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (2) means a feature was introduced in 12.1(2)T. If a cell in this column is empty, the feature was included in the initial base release.

Note These feature set tables contain only the features specific to the T-train. For a more complete list of features, see the feature set tables in the mainline release notes on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121relnt/xprn121/121feats.htm.

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

		Feature Sets					
Features	**In**	**IP**	**IP Plus**	**IP Plus IPSEC 56**	**IP/FW/IDS**	**IP/FW/ IDS Plus IPSec 56**	**IP/IPX**
IP Multicast							
Bidirectional PIM	(2)	No	Yes	Yes	No	Yes	No
IP Routing Protocols							
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous							
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes	Yes
DiffServ Compliant Weighted Random Early Detection	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Fax Relay Packet Loss Concealment	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Implementing DiffServ for End-to-End Quality of Service	(5)	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Tunnel Management Enhancementss	(5)	No	Yes	Yes	No	Yes	No
L2TP Tunnel Switching	(5)	No	Yes	Yes	No	Yes	No
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	(5)	No	Yes	Yes	No	Yes	No
Parser Cache	(5)	No	Yes	Yes	No	Yes	No
RSVP Support for Frame Relay	(5)	No	Yes	Yes	No	Yes	No

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

		Feature Sets					
Features	**In**	**IP**	**IP Plus**	**IP Plus IPSEC 56**	**IP/FW/IDS**	**IP/FW/ IDS Plus IPSec 56**	**IP/IPX**
SDLC SNRM Timer and Window Size Enhancements	(5)	No	No	No	No	No	No
UDLR Tunnel ARP and IGMP Proxy	(5)	No	Yes	Yes	No	Yes	No
VoIP Call Admission Control using RSVP	(5)	No	No	No	No	No	No
Multimedia and Quality of Service							
H.323 V2 Enhancements	(3)	No	No	No	No	No	No
Quality of Service Voice Enhancements	(3)	No	No	No	No	No	No
Multiservice Applications							
Voice over Frame Relay (Cisco 1750 only)	(2)	No	No	No	No	No	No
Security							
Secure Shell Version 1 Integrated Client	(3)	No	No	Yes	No	Yes	No
SSH Version 1 Server Support		No	No	Yes	No	Yes	No
Virtual Private Network (VPN) Module for the Cisco 1700 Series	(2)	No	No	Yes	No	Yes	No
WAN							
Frame Relay Switching Enhancements: Shaping and Policing	(2)	No	Yes	Yes	No	Yes	No

Table 3 Feature List by Feature Set for the Cisco 1700 Series, Part 2

		Feature Sets					
Features	**In**	**IP/IPX/FW/ IDS Plus**	**IP/IPX/AT/ IBM**	**IP/IPX/AT/ IBM Plus**	**IP/Voice Plus IPSEC 56**	**IP/Voice/ FW/IDS Plus**	**IP/Voice/ FW/IDS Plus IPSec 56**
IP Multicast							
Bidirectional PIM	(2)	Yes	No	Yes	Yes	Yes	Yes
IP Routing Protocols							
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous							
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes	Yes
DiffServ Compliant Weighted Random Early Detection	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Fax Relay Packet Loss Concealment	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Implementing DiffServ for End-to-End Quality of Service	(5)	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Tunnel Management Enhancementss	(5)	Yes	No	Yes	Yes	Yes	Yes
L2TP Tunnel Switching	(5)	Yes	No	Yes	Yes	Yes	Yes
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	No	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	No	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	No	Yes	Yes	No	No	No
UDLR Tunnel ARP and IGMP Proxy	(5)	Yes	No	Yes	Yes	Yes	Yes
VoIP Call Admission Control using RSVP	(5)	No	No	No	Yes	Yes	Yes
Multimedia and Quality of Service							
H.323 V2 Enhancements	(3)	No	No	No	Yes	Yes	Yes
Quality of Service Voice Enhancements	(3)	No	No	No	Yes	Yes	Yes
Multiservice Applications							

Table 3 Feature List by Feature Set for the Cisco 1700 Series, Part 2 (continued)

		Feature Sets					
Features	**In**	**IP/IPX/FW/ IDS Plus**	**IP/IPX/AT/ IBM**	**IP/IPX/AT/ IBM Plus**	**IP/Voice Plus IPSEC 56**	**IP/Voice/ FW/IDS Plus**	**IP/Voice/ FW/IDS Plus IPSec 56**
Voice over Frame Relay (Cisco 1750 only)	(2)	No	No	No	Yes	Yes	Yes
Security							
Secure Shell Version 1 Integrated Client	(3)	No	No	No	Yes	No	Yes
SSH Version 1 Server Support		No	No	No	Yes	No	Yes
Virtual Private Network (VPN) Module for the Cisco 1700 Series	(2)	No	No	No	Yes	No	Yes
WAN							
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	No	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 1700 Series, Part 3

		Feature Sets				
Features	**In**	**IP/IPX/Voice/ FW/IDS Plus**	**IP Plus IPSEC 3DES**	**IP/FW/IDS Plus IPSec 3DES**	**IP/Voice Plus IPSEC 3DES**	**IP/Voice/FW/ IDS Plus IPSec 3DES**
IP Multicast						
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes	Yes
IP Routing Protocols						
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes
Miscellaneous						
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes
DiffServ Compliant Weighted Random Early Detection	(5)	Yes	Yes	Yes	Yes	Yes
Fax Relay Packet Loss Concealment	(5)	Yes	Yes	Yes	Yes	Yes
Implementing DiffServ for End-to-End Quality of Service	(5)	Yes	Yes	Yes	Yes	Yes
L2TP Tunnel Management Enhancementss	(5)	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 1700 Series, Part 3 (continued)

		Feature Sets				
Features	**In**	**IP/IPX/Voice/ FW/IDS Plus**	**IP Plus IPSEC 3DES**	**IP/FW/IDS Plus IPSec 3DES**	**IP/Voice Plus IPSEC 3DES**	**IP/Voice/FW/ IDS Plus IPSec 3DES**
L2TP Tunnel Switching	(5)	Yes	Yes	Yes	Yes	Yes
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	No	No	No	No	No
UDLR Tunnel ARP and IGMP Proxy	(5)	Yes	Yes	Yes	Yes	Yes
VoIP Call Admission Control using RSVP	(5)	Yes	No	No	Yes	Yes
Multimedia and Quality of Service						
H.323 V2 Enhancements	(3)	Yes	No	No	Yes	Yes
Quality of Service Voice Enhancements	(3)	Yes	No	No	Yes	Yes
Multiservice Applications						
Voice over Frame Relay (Cisco 1750 only)	(2)	Yes	No	No	Yes	Yes
Security						
Secure Shell Version 1 Integrated Client	(3)	No	Yes	Yes	Yes	Yes
SSH Version 1 Server Support		No	Yes	Yes	Yes	Yes
Virtual Private Network (VPN) Module for the Cisco 1700 Series	(2)	No	Yes	Yes	Yes	Yes
WAN						
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1700 series routers for Release 12.1 T.

New Hardware Features in Release 12.1(5)T

VIC-2FXO-M3 Support on the Cisco 1750

The Australian version of the two-port Foreign Exchange Office (FXO) voice/fax interface card for the voice/fax network module (VIC-2FXO-M3) is supported by the Cisco 1750 in Cisco IOS Release 12.1(5)T.

New Software Features in Cisco IOS Release 12.1(5)T

The following new software features are supported by the Cisco 1700 series routers for Release 12.1(5)T:

AutoInstall Using DHCP for LAN Interfaces

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature which provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. In Cisco IOS release 12.1(5)T, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI interfaces. Prior to this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also allows the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. Additionally, this feature allows for the uploading of configuration files using unicast TFTP. For further details, please see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_dhcpa.htm

Closed User Group Selection Facility Suppress Option

A closed user group (CUG) selection facility is a specific encoding element that allows a destination data terminal equipment (DTE) to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 data communications equipment (DCE) interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA).

DiffServ Compliant Weighted Random Early Detection

This feature extends the functionality of WRED (Weighted Random Early Detection) to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). This feature enables WRED to be compliant with the DiffServ standard and the AF PHB standard being developed by the Internet Engineering Task Force (IETF). This feature enables customers to implement AF PHB by coloring packets according to DSCP values and then assigning preferential drop probabilities to those packets.This feature adds two new commands, **random-detect dscp** and **dscp**. It also adds two new arguments, *dscp-based* and *prec-based***,** to two existing WRED-related commands—the **random-detect** (interface) command and the **random-detect-group** command.

Fax Relay Packet Loss Concealment

This feature improves the current real-time fax over Internet Protocol (IP) (known as fax relay) implementation in Cisco gateways so that fax transmissions work reliably over higher packet-loss conditions.

This feature also includes enhanced real-time fax debugging capabilities and statistics. These features give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.

These improvements include configuration of fax relay ECM (Error Correction Mode) on the voice over IP (VoIP) dial peer. ECM provides for error-free page transmission. This mode is available on fax machines that include memory for storage of the page data (usually high-end fax machines).

Implementing DiffServ for End-to-End Quality of Service

Differentiated services (DiffServ) describes a set of end-to-end quality of service (QoS) capabilities. End-to-end QoS means that the network can deliver service required by specific network traffic from one end of the network to another. Cisco IOS QoS software supports three types of service models: best-effort, integrated (IntServ), and differentiated services (DiffServ).

For more information about the best-effort and integrated-service models, see the *Cisco IOS Quality of Service Solution Configuration Guide.*

Differentiated services is a multiple service model that satisfies different QoS requirements. The network tries to deliver service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit Differentiated Services Code Point (DSCP) setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, police traffic, and perform intelligent queueing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Cisco IOS QoS includes the following features that support differentiated services:

- Committed access rate (CAR), which performs packet classification through IP precedence and QoS group settings. CAR performs metering and policing of traffic, providing bandwidth management.
- Intelligent queueing schemes such as Weighted Random Early Detection (WRED) and Weighted Fair Queueing (WFQ) and their equivalent features on the Versatile Interface Processor (VIP), which are VIP-distributed WRED services.
- Modular QoS Command-Line Interface (MQC) so that you can specify a traffic class independently of QoS policies.

- Low Latency Queueing (LLQ) brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be unqueued and sent first (before packets in other queues are unqueued), giving delay-sensitive data preferential treatment over other traffic.
- Generic Traffic Shaping (GTS) shapes traffic by reducing outbound traffic flow to avoid congestion. It constrains traffic to a particular bit rate by using the token bucket mechanism. GTS applies on a per-interface basis and can use access lists to select the traffic to shape.

For more information about Cisco IOS QoS features, see the *Cisco IOS Quality of Service Solutions Guide* and the *Cisco IOS Quality of Service Command Reference*.

NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)

Microsoft NetMeeting is a Windows-based application that enables multi-user interaction and collaboration from a users PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made.

NTP MIB

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a Network Management System (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table. For complete details on the Cisco implementation of the NTP MIB, see the MIB file itself ("CISCO-NTP-MIB.my", available through Cisco.com at http://www.cisco.com/public/mibs/v2/).

Parser Cache

The Parser Cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files. This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuation lines which differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on). Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

The parser cache is enabled by default on all platforms using Cisco IOS 12.1(5)T or later. A new command, **[no] parser cache**, allows the disabling or re-enabling of this feature.

RSVP Support for Frame Relay

Queueing manages congestion on a router interface or a virtual circuit (VC). In a Frame Relay environment, the congestion point may not be the interface itself, but it may be the VC because of the committed information rate (CIR). For real-time traffic (voice flows) to be transmitted in a timely manner, the data rate must not exceed the CIR or packets might be dropped causing voice quality issues. Frame Relay traffic shaping (FRTS) is configured on the interfaces to control the outbound traffic rate by preventing the router from exceeding the CIR. This means that fancy queueing such as class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), and weighted fair queueing (WFQ), can run on the VC to provide the quality of service (QoS) guarantees for the traffic.

Previously, RSVP reservations were not constrained by the CIR of the flow's outbound VC. As a result, oversubscription could occur when the sum of the RSVP traffic and other traffic exceeded the CIR.

The RSVP support for Frame Relay feature allows RSVP to work with per VC (data link connection identifier (DLCI)) queueing for voice-like flows. Traffic shaping must be enabled in a Frame Relay environment for accurate admission control of resources (bandwidth and queues) at the congestion point; that is, the VC itself. Specifically, RSVP can work with VCs defined at the interface and subinterface levels. There is no limit to the number of VCs that can be configured per interface or subinterface.

SDLC SNRM Timer and Window Size Enhancements

The SDLC SNRM Timer and Window Size Enhancements feature introduces a new window size setting for SDLC configurations, and a new timeout setting for the SNRM frame. These enhancements change the operation of SDLC processing on a multidrop line.

Window Size Setting

Prior to this feature, all SDLC addresses on the multidrop had the same window count. Now the window count can be configured on a Physical Unit (PU) or SDLC address level. This enhancement gives a controller a different window size than other devices on the interface, and allows devices attached to the multidrop to be sized individually.

Timeout Setting for SNRM frame

Cisco IOS software SDLC implementation currently utilizes a common response timer (T1) for all outstanding commands. Calculating the maximum frame size and line speed produces a minimum time of 3.5 seconds for receiving acknowledgments; thus, polling stations used for link activation utilize this 3.5-second timer. This is a problem on a multidrop, because stations that do not respond to the SNRM will have 3.5 seconds of downtime-waiting before the next station that is active is polled. This enhancement reduces the time to stations that are waiting idle, as opposed to those that are active.

UDLR Tunnel ARP and IGMP Proxy

Most protocols in the Internet assume that links are bidirectional. In particular, routing protocols used by directly connected routers no longer behave properly in the presence of a unidirectional link, such as a satellite link. The Unidirectional Link Routing feature, introduced in Cisco IOS Release 12.0(3)T, enables a router to emulate the behavior of a bidirectional link for operation of IP over unidirectional links.

The unidirectional link routing (UDLR) enhancements introduced in Cisco IOS Release 12.1(5)T include enhancements to the existing UDLR tunnel mechanism and the addition of the Internet Group Management Protocol (IGMP) proxy mechanism.

VoIP Call Admission Control using RSVP

The VoIP Call Admission Control using the Resource Reservation Protocol (RSVP) feature synchronizes with H.323 Version 2 (Fast Connect) setup procedures to guarantee that the required QoS for VoIP calls is maintained across the IP network. Before Cisco IOS Release 12.1(3)XI, VoIP gateways used H.323 Version 1 (Slow Connect) procedures when initiating calls requiring bandwidth reservation. This feature, which is enabled by default, allows gateways to use H.323 Version 2 (Fast Connect) for all calls, including those requiring RSVP.

New Software Features in Cisco IOS Release 12.1(3)T

The following new software features are supported by the Cisco 1700 series routers for Release 12.1(3)T:

H.323 Version 2 Enhancements for the Cisco 1750 Router

For the Cisco 1750 router, these enhancements provide compliance with all mandatory elements of H.323 Version 2 for the Cisco IOS based Gateway, Gatekeeper, and Proxy products. Along with other selected features, they provide critical new functionality needed for interoperablilty and network deployment. New features include:

- V2 Compliant GW/GK/Proxy
- Lightweight registration
- Resource Availability Indication (RAS v2)
- DTMF Digit relay via H.245 User Information Element
- Enhanced GK selection algorithm for Gateways
- Single Proxy Scenario
- GW Registration of E.164 addresses for FXS
- Tunneling of QSIG Supplementary Services via H.225 UUIE
- Gateway support for tunneling of Redirecting Number Information Elements in H.225 messages

Quality of Service Voice Enhancements

Cisco IOS Release 12.1(3)T supports the following features:

- Low Latency Queuing for Voice over Frame Relay
- H.323 voice (v2) support
- Registration, admission, and status protocol (RAS) voice (v2) enhancement support
- DiffServ
- Fax relay enhancements

To configure these features on Cisco 1700 series routers, see the online document *Quality of Service Solutions Configuration Guide*. From Cisco.com, click on the path (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Configuration Guides and Command References**: **Configuration Guides and Command References**: **Quality of Service Solutions Configuration Guide**

Secure Shell Version 1 Integrated Client

Secure Shell (SSH) is a protocol that provides a secure remote connection to another router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The Secure Shell Version 1 Integrated Client feature is an application running over TCP/IP to provide strong authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication.

The SSH client functionality is available only when the SSH server is enabled.

New Software Features in Cisco IOS Release 12.1(2)T

The following new software features are supported by the Cisco 1700 series routers for Release 12.1(2)T:

Bidirectional PIM

Bidir-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode
- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is only routed along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

Membership to a bidirectional group is signalled via explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

Bidir-PIM is derived from the mechanisms of PIM sparse mode (PIM SM) and shares many SPT operations. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Frame Relay Switching Enhancements: Shaping and Policing

The Frame Relay Switching Enhancements feature enables a router in a Frame Relay network to be used as a Frame Relay switch.

This feature includes the following Frame Relay switching enhancements:

- Traffic Shaping on Switched PVCs
- Frame Relay Switching over ISDN B Channels
- Traffic Policing on UNI DCE
- Congestion Management on Switched PVCs

Before the Frame Relay Switching Enhancements feature was introduced, routers had limited Frame Relay switching functionality. With this feature, a router acting as a virtual Frame Relay switch can be configured to do the following:

- Apply Frame Relay traffic shaping functionality to switched PVCs, enabling the router to act as a Frame Relay port concentrator.
- Support ISDN interfaces in addition to serial interfaces.
- Discard switched packets with the DE bit set when there is network congestion.
- Police incoming traffic to ensure adherence to service contracts.
- Set the Forward/Backward Explicit Congestion Notification (FECN/BECN) bits in switched packets when there is network congestion.

OSPF Flooding Reduction

The explosive growth of the Internet has placed the focus on the scalability of Interior Gateway Protocols such as OSPF. The networks using OSPF are becoming larger every day and will continue to expand to accommodate the demand to connect to the Internet.

Internet Service Providers and customers with large networks have regularly complained that OSPF has a traffic overhead, even when the network topology is stable.

By design, OSPF requires link-state advertisements (LSAs) to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 min to around 50 min or so.

This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF Flooding Reduction feature works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set, thus making them DoNotAge (DNA) LSAs.

Virtual Private Network (VPN) Module for the Cisco 1700 Series

The Cisco 1700 series routers, which includes the Cisco 1720 and 1750 models, are modular access routers for small and medium businesses and small branch offices. Cisco 1700 routers deliver routing, firewall, and VPN functions for Internet data and voice applications.

The VPN module, which fits into a slot inside the Cisco 1720 or 1750 chassis, assists the host processor by accelerating layer 3 IP Security (IPSec) data and voice encryption and decryption. The VPN module supports DES and 3DES encryption algorithms, MD5 and SHA-1 hashing, and Diffie-Hellman key generation.

The VPN module encrypts data using DES and 3DES algorithms at speeds suitable for full duplex T1/E1 serial connections (4 megabits per second for 1518-byte packets). Equipped with a VPN module, a Cisco 1700 router supports up to 100 encrypted tunnels for concurrent sessions with mobile users or other sites.

Voice Over Frame Relay

Voice over Frame Relay (VoFR) enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. Configuration information is available in the “Cisco IOS Multiservice Applications Configuration Guide” and “Cisco IOS Multiservice Applications Command Reference” publications.

Before configuring VoFR on a router, you must configure your Frame Relay backbone network. As part of your Frame Relay configuration, you need to configure the map class, and the Local Management Interface (LMI) among other Frame Relay functionality. For more information about Frame Relay configuration, refer to the "Cisco IOS Wide-Area Networking Configuration Guide."

The Cisco VoFR implementation allows the following types of VoFR calls:

- Static FRF.11 trunks
- Switched VoFR calls:
  - Dynamic switched calls
  - Cisco-trunk (private line) calls

New Software Features in Cisco IOS Release 12.1(1)T

The following new software features are supported by the Cisco 1700 series routers for Release 12.1(1)T:

SSH Version 1 Server Support

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

H.323 V2 Enhancements

Cisco H.323 Version 2 Phase 2 enhancements upgrade several optional features of the H.323 Version 2 specification, and facilitate customized extensions to the Cisco Gatekeeper.

- H.323v2 Fast Connect—The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing before endpoint connections can be established.
- H.245 Tunneling—Through H.245 tunneling, H.245 messages are encapsulated within Q.931 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any Q.931 message. H.245 tunneling is not supported as a stand-alone feature; initiation of H.245 tunneling procedures can be initiated only by using the **dtmf-relay** command, and only from an active Fast Connect call. Furthermore, if **dtmf-relay** is configured on a Version 2 VoIP dial peer and the active call has been established by using Fast Connect, tunneling procedures initiated by the opposite endpoint are accepted and supported.

  H.245 tunneling is backward compatible with H.323 Version 1 configurations.
- H.450.2 Call Transfer—Call Transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco gateways support H.450.2 Call Transfer as the transferred and transferred-to party. The transferring endpoint must be an H.450-capable terminal; the Cisco gateway cannot act as the transferring endpoint. Gatekeeper-controlled or Gatekeeper-initiated Call Transfer is not supported.

Note Certain devices are limited in their support of H.450. The Cisco 1700 and ubr820 platforms do not support Interactive Voice Response (IVR). Therefore, these platforms are not able to act as H.450 Transferring endpoints.

- H.450.3 Call Deflection—Call Deflection is a feature under H.450.3 Call Diversion (Call Forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 Call Deflection as the originating, deflecting, and deflected-to gateway. The Cisco gateway as the deflecting gateway will support invocation of Call Deflection only by using an incoming PRI QSIG message (a Call Deflection cannot be invoked by using any other trunk type).
- Hookflash Relay—A “hookflash” indication is a brief on-hook condition during a call. The indication is not long enough in duration to be interpreted as a signal to disconnect the call. You can create a hookflash indication by quickly depressing and releasing the hook on your telephone.
- H.235 Security—Security for Registration, Admission, and Status protocol (RAS) signaling between H.323 endpoints and Gatekeepers is enhanced in H.323 Version 2 Phase 2 by including secure endpoint registration of the Cisco gateway to the Cisco Gatekeeper and secure per-call authentication. The authentication type is “password with hashing” as described in ITU H.235. Specifically, the encryption method is MD5 with password hashing. This functionality is provided by the security token required-for CLI on the Gatekeeper and the security password CLI on the gateway.
- GKTMP—The Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco Gatekeeper provides a transaction-oriented application protocol that allows an external application to modify Gatekeeper behavior by processing specified RAS messages.
- Gateway Support for Alternate Endpoints—The Alternate Endpoint feature allows a Gatekeeper to specify alternative destinations for a call when queried with an Admission Request (ARQ) by an originating gateway. If the first destination gateway fails to connect, the Gatekeeper tries all the alternate destinations before going to the next dial peer rotary (if a rotary is configured).
- Gateway Support for a Network-Based Billing Number—This feature informs the Gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the Admission Request (ARQ) message sent by the ingress gateway. No configuration is necessary for this feature.

- Gateway Support for Voice-Port Description—This feature provides the Gatekeeper with a configurable string that identifies the voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the ARQ message sent by the ingress gateway. The string in the ARQ corresponds to the setting of the voice-port description command.

Limitations and Restrictions

MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 5.

Table 5 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be decided
OLD-CISCO-DECNET-MIB	To be decided
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be decided
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be decided
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be decided

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. If you have an account with Cisco.com, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit,* go to Cisco.com, press **Login**, and click to **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.1 T that can apply to the Cisco 1700 series routers.

Last Maintenance Release of Cisco IOS Release 12.1 T

The last maintenance release of the 12.1 T release train is 12.1(5)T. The migration path for customers who need bug fixes for the 12.1 T features is the 12.2 mainline release. The 12.2 mainline release has the complete feature content of 12.1 T and will eventually reach general deployment (GD).

The last maintenance release was renamed from 12.1(4)T to 12.1(5)T to synchronize with its parent software base, the 12.1(5) mainline release, and to reflect that 12.1(5)T has all the bug fixes of the 12.1(5) mainline release. The 12.1 T release train is a superset of the 12.1 mainline release; hence any defect fixed in the 12.1 mainline is also fixed in 12.1 T. The set of features for 12.1(4)T is the same as that for 12.1(5)T. There was no change in the feature content of the release. The release was renamed so that the releases would be consistent with the Cisco release process.

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 .

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:**).

Fan Operation in Cisco 1700 Series Routers

Be advised that the fans in the Cisco 1700 series routers stay off until thermally activated (45˚C/115˚F).

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 **show flash ?**. This will list all of the valid partitions. Then enter **show flash:xx: all** on each valid partition.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T*.

All caveats in Cisco IOS Release 12.1 are also in Cisco IOS Release 12.1 T.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and is located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login.** Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools.

Caveats for Release 12.1(3)T

This section describes possibly unexpected behavior by Release12.1(3)T, specific to the Cisco 1750 router only. The following caveats are severity 3.

CSCdr39864

The Cisco 1750 router is a Residential Gateway (RGW) and supports MGCP on FXS ports only, therefore, do not configure MGCP on FXO or E&M ports.

CSCdr26084

From the perspective of the Cisco 1750 router command line interface (CLI), the format used to describe the slot and port is <slot>/<port>. However, after executing the command **show mgcp endpoint**, the Cisco 1750 router might display the output in the format <slot>/<subinterface>/<port>, such as 0/0/1 for port 0/1. The 0 digit for the <slot> does not represent hardware; it is a phantom number added by Cisco 1750 internal code because there is no concept of a subinterface for Cisco 1750 routers. This syntax structure matches that of some other networking equipment requiring unique specifications for all three hardware aspects:the slot number, the sub-unit number, and the port number. On the Cisco 1750 router, the <subinterface> is actually the slot number. The output format of the command **show mgcp endpoint** thus provides information about how to configure the command **call agent**.

Caveats for Release 12.1(1)T

This section describes possibly unexpected behavior by Release12.1(1)T, specific to the Cisco 1700 series routers. Only severity 1 and 2 caveats are included.

CSCdp97036

The Australian variant of the two-port Foreign Exchange Office (FXO) voice/fax interface card for the voice/fax network module (VIC-2FXO-M3) is not supported by the Cisco 1750 at this time.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. 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 these documents:

- Release-Specific Documents, page 24
- Platform-Specific Documents, page 25
- Feature Modules, page 26
- Cisco IOS Software Documentation Set, page 26

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.1 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.1: Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.1*

  See *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.1 and Release 12.1 T.

On Cisco.com at:

Technical Documents: Documentation Home Page: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Caveats**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.1**: **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. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools.

Platform-Specific Documents

Cisco 1720 Router

These individual and groups of documents are available for the Cisco 1720 router on Cisco.com and the Documentation CD-ROM:

- *Installing Your Cisco 1720*
- *Cisco 1720 Router Hardware Installation Guide*
- *Cisco 1700 Router Software Configuration Guide*
- *Regulatory Compliance and Safety Information*
- Configuration notes
- Release notes for the Cisco 1720 router
- *WAN Interface Cards Hardware Installation Guide*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1720 Router

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1720 Router

Cisco 1750 Router

These individual and groups of documents are available for the Cisco 1750 router on Cisco.com and the Documentation CD-ROM:

- *Cisco 1750 Router Hardware Installation Guide*
- *Voice-over-IP Quick Start Guide*
- Cisco 1750 software configuration guides
- *Cisco WAN Interface Cards Hardware Installation Guide*

- *Installing and Removing Packet Voice DSP Modules Configuration Note*
- Release notes for the Cisco 1750 router
- Safety information for Cisco 1600 and 1700 routers

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1750 Router

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1750 Router

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1 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 Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: **Cisco IOS Release 12.1**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.1**: **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 Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

Cisco IOS Release 12.1 Documentation Set

Table 6 describes the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form ordered.

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.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1

Table 6 Cisco IOS Software Release 12.1 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume I* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
• *Cisco IOS Dial Services Configuration Guide: Terminal Services* • *Cisco IOS Dial Services Configuration Guide: Network Services* • *Cisco IOS Dial Services Command Reference*	Preparing for Dial Access Modem Configuration and Management ISDN and Signalling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios

Table 6 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	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 and Novell IPX Overview Configuring AppleTalk Configuring 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, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Voice Video Broadband
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 6 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
- *Cisco IOS Wide-Area Networking Configuration Guide* - *Cisco IOS Wide-Area Networking Command Reference*	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
- *New Features in 12.1-Based Limited Lifetime Releases* - *New Features in Release 12.1 T* - Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms) - *Cisco IOS Debug Command Reference* - *Cisco IOS Dial Services Quick Configuration Guide*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. If you have an account with Cisco.com, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to CC, press **Login**, and click to **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
- 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 24.