



Release Notes for Cisco 2500 Series Routers for Cisco IOS Release 12.1 T

November 27, 2000



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 2500 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:

- Early Deployment Releases, page 2
- System Requirements, page 2
- New and Changed Information, page 11
- Limitations and Restrictions, page 20
- Important Notes, page 21
- Caveats, page 22
- Related Documentation, page 23
- Obtaining Documentation, page 28
- Obtaining Technical Assistance, page 28



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

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

78-10843-04

Early Deployment Releases

These release notes describe the Cisco 2500 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 lists shows the recent early deployment releases of the Cisco 2500 series routers:

- Release 11.2 P, up to 11.2(21)P
- Release 11.3 T, up to 11.3(11)T
- Release 12.0 T, up to 12.0(7)T
- Release 12.1 T, up to 12.1(5)T

For more information, see the “Platform-Specific Documents” section on page 24 about accessing related release note documents.

System Requirements

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

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Software Release, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for Cisco 2500 Series Routers

Feature Sets	Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
IP Feature Sets	IP	c2500-i-1	16 MB	10 MB	Flash
	IP/FW	c2500-io-1	16 MB	10 ¹ MB	Flash
	IP/FW Plus IPSec 56	c2500-ios56i-1	16 MB	10 MB	Flash
	IP Plus	c2500-is-1	16 MB	10 MB	Flash
	IP Plus IPSec 56	c2500-is56i-1	16 MB	10 MB	Flash
	IP/H323	c2500-ix-1	16 MB	16 MB	Flash
	IP/IBM/SNASW	c2500-a3i3r4-1	16 MB	16 MB	Flash
	IP/IPX/AT/DEC	c2500-d-1	16 MB	8 MB	Flash
	IP/IPX/AT/DEC/FW Plus	c2500-dos-1	16 MB	10 MB	Flash
	IP/IPX/AT/DEC Plus	c2500-ds-1	16 MB	8 MB	Flash

Table 1 Memory Requirements for Cisco 2500 Series Routers (continued)

Feature Sets	Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Enterprise Feature Sets	Enterprise/FW Plus IPSec 56	c2500-jos56i-1	16 MB	16 MB	Flash
	Enterprise Plus	c2500-js-1	16 MB	16 MB	Flash
	Enterprise Plus IPSec 56	c2500-js56i-1	16 MB	16 MB	Flash
FRAD Feature Sets	FRAD	c2500-f-1	8 MB	8 MB	Flash
	LAN FRAD/OSPF	c2500-f2in-1	8 MB	8 MB	Flash
	LAN FRAD	c2500-fin-1	8 MB	8 MB	Flash
	Remote Access Server (RAS)	c2500-c-1	16 MB	8 MB	Flash
	ISDN	c2500-g-1	8 MB	8 MB	Flash
	Service Provider with PT/TARP ²	c2500-p7-1	8 MB	4 MB	Flash

1. 16 MB in Release 12.1(1)T.

2. This image was introduced in Cisco IOS Release 12.1(3)T. It is not supported in previous releases.

Hardware Supported

Cisco IOS Release 12.1 T supports the Cisco 2500 series routers:

- Single LAN routers—Models 2502, 2503, 2504, 2520, 2521, 2522 and 2523
- Mission-specific, entry-level routers—Models 2501CF, 2502CF, 2503I, 2504I, 2520CF, 2520LF, 2521CF, 2521LF, 2522CF, 2522LF, 2523CF and 2523LF
- Router/hub combinations—Models 2505, 2507 and 2516
- Access servers—Models 2509 to 2512
- Dual LAN routers—Models 2513, 2514 and 2515
- Modular routers—Models 2524 and 2525 (optional integrated DSU/CSU or NT-1)

For detailed descriptions of the new hardware features, see “New and Changed Information” section on page 11.

Table 2 Supported Interfaces for the Cisco 2500 Series

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
LAN Interfaces	Ethernet (AUI)	Cisco 2501, 2503, 2509, 2511, 2513, 2514, 2520, 2522, and 2524 only
	Ethernet (10BaseT)	Cisco 2505, 2507, 2516, and 2524 only
	4-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only
	16-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only

Table 2 Supported Interfaces for the Cisco 2500 Series (continued)

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
WAN Data Rates	48/56/64 kbps	Cisco 2500 series
	128 kbps	Cisco 2500 series
	1.544/2.048 Mbps	Cisco 2500 series
WAN Interfaces	EIA/TIA-232	Cisco 2500 series
	EIA/TIA-449	Cisco 2500 series
	EIA-530	Cisco 2500 series
	X.21	Cisco 2500 series
	V.35	Cisco 2500 series
	Serial, synchronous	Cisco 2500 series
	Serial, synchronous, and asynchronous	Cisco 2520, 2521, 2522, and 2523 only
	ISDN BRI S/T	Cisco 2503, 2504, 2516, 2520, 2521, 2522, 2523, 2524, and 2525 only
	ISDN BRI U	Cisco 2524 and 2525 only

Determining the Software Release

To determine the version of Cisco IOS software running on your Cisco 2500 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 (C2500-DOS-L), Version 12.1(5)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/cisco/mkt/ios/prodlit/957_pp.htm

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 2500 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 3, Table 4, and Table 5 list the features and feature sets supported by the Cisco 2500 series routers in Cisco IOS Release 12.1 T and 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 3 Feature List by Feature Set for the Cisco 2500 Series, Part 1

Features	In	Feature Sets					
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus IPSec 56	IP/H323
Configuration Fundamentals							
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast							
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing Protocols							
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Management							
Service Assurance Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous							

Table 3 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

Features	In	Feature Sets					
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus IPSec 56	IP/H323
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Class-Based Quality of Service Management Information Base	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes	Yes
IGMP Version 3	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Enhanced H.225/H.245 Forwarding Engine	(5)	No	Yes	Yes	No	No	No
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Support of H.323 v2 Call Signalling (FastConnect)	(5)	No	Yes	Yes	No	No	No
NAT - Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	No	No	Yes	Yes	Yes	No
State-Refresh		Yes	Yes	Yes	Yes	Yes	Yes
Multiservice Applications—Voice							
Gatekeeper to Gatekeeper Redundancy and Load-Sharing	(2)	No	No	No	No	No	Yes
Quality of Service							
Express Resource Transport Protocol and TCP Header Compression (CRTP)		Yes	Yes	Yes	Yes	Yes	Yes
Reliability							
Pragmatic General Multicast (PGM)		No	No	No	No	No	No
WAN							

Table 3 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

Features	In	Feature Sets					
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus IPSec 56	IP/H323
Frame Relay ILMI Address Registration	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 2

Features	In	Feature Sets					
		IP/IBM/ SNASW	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ FW Plus IPSec 56	Enterprise Plus
Configuration Fundamentals							
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast							
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing Protocols							
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes
Management							
Service Assurance Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous							
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Class-Based Quality of Service Management Information Base	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes	Yes
IGMP Version 3	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Enhanced H.225/H.245 Forwarding Engine	(5)	No	No	Yes	No	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

Features	In	Feature Sets					
		IP/IBM/ SNASW	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ FW Plus IPSec 56	Enterprise Plus
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Support of H.323 v2 Call Signalling (FastConnect)	(5)	No	No	Yes	No	Yes	Yes
NAT - Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	No	Yes	Yes	Yes	Yes
State-Refresh		Yes	Yes	Yes	Yes	Yes	Yes
Multiservice Applications—Voice							
Gatekeeper to Gatekeeper Redundancy and Load-Sharing	(2)	No	No	No	No	No	No
Quality of Service							
Express Resource Transport Protocol and TCP Header Compression (CRTP)		Yes	Yes	Yes	Yes	Yes	Yes
Reliability							
Pragmatic General Multicast (PGM)		No	No	No	No	Yes	Yes
WAN							
Frame Relay ILMI Address Registration	(3)	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 3

Features		Feature Sets						
		Enter- prise Plus IPSec 56	FRAD	LAN FRAD/ OSPF	LAN FRAD	Remote Access Server (RAS)	ISDN	Service Provider with PT/TARP ¹
Configuration Fundamentals								
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast								
Bidirectional PIM	(2)	Yes	No	No	No	No	No	Yes
Source Specific Multicast	(3)	Yes	No	No	No	Yes	Yes	Yes
IP Routing Protocols								
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management								
Service Assurance Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous								
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	No	No	Yes	Yes	Yes
Class-Based Quality of Service Management Information Base	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	(5)	Yes	No	No	No	Yes	No	Yes
IGMP Version 3	(5)	Yes	No	No	No	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	No	No	No	No	No	No
NAT - Support for NetMeeting Directory (Internet Locator Service - ILS)	(5)	Yes	No	No	No	Yes	No	No
NAT - Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	No	No	No	No	No	No
NAT - Support of IP Phone to Cisco Call Manager	(5)	Yes	No	No	No	Yes	No	No
NTP MIB	(5)	Yes	No	No	No	Yes	No	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	No	No	No	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features		Feature Sets						
		Enterprise Plus IPSec 56	FRAD	LAN FRAD/ OSPF	LAN FRAD	Remote Access Server (RAS)	ISDN	Service Provider with PT/TARP ¹
Router-Port Group Management Protocol	(5)	Yes	No	No	No	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes	No	No	No
State-Refresh		Yes	No	No	No	Yes	Yes	Yes
Multiservice Applications—Voice								
Gatekeeper to Gatekeeper Redundancy and Load-Sharing	(2)	No	No	No	No	No	No	Yes
Quality of Service								
Express Resource Transport Protocol and TCP Header Compression (CRTP)		Yes	No	No	No	Yes	No	Yes
Reliability								
Pragmatic General Multicast (PGM)		Yes	No	No	No	No	No	Yes
WAN								
Frame Relay ILMI Address Registration	(3)	Yes	Yes	Yes	Yes	Yes	No	Yes
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1. This image was introduced in Cisco IOS Release 12.1(3)T. It is not supported in previous releases.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 2500 series routers for Release 12.1 T.

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

The following new software features are supported by the Cisco 2500 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

Class-Based Quality of Service Management Information Base

The Class-Based Quality of Service Management Information Base (Class-Based QoS MIB) provides read access to class-based QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS CLI, including information regarding class map and policy map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

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).

Dial-on-Demand Authentication Enhancements

The following enhancements to dial-on-demand authentication are provided with this feature:

- The NAS IP address plus a configured suffix can be sent to the RADIUS server as a username for authentication.
- A password other than the default password “cisco” can be sent to the RADIUS server for authentication.
- The username for two-way authentication will be specified by a new VSA, “outbound:send-name=<string>”.

This feature also introduces modifications to the **dialer aaa** command, which provides username configuration capability for dial-on-demand.

DFP Support in DistributedDirector—Cisco 2501 and Cisco 2502 Only

This protocol allows the user to configure the DistributedDirector to communicate with various DFP agents. The DistributedDirector tells the DFP agents how often they should report load information; then the DFP agents can tell the DistributedDirector which LocalDirector cluster to remove from providing service.

IGMP Version 3

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) adds support for “source filtering” which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host (or by other routers via Protocol Independent Multicast (PIM)) to that network. In addition to restricting traffic on the network of the receiver host, IGMPv3 membership information may also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source Specific Multicast feature, introduced in Cisco IOS Release 12.1(5)T, hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases where IGMPv3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable Source Specific Multicast (SSM): URL Rendezvous Directory (URD) and IGMP v3lite. Both of these features were introduced with SSM in Cisco IOS Release 12.1(3)T.

Interface Index Persistence

One of the most commonly used identifiers used in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the “name” of the interface. Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

Cisco IOS Release 12.1(5)T adds support for an ifIndex value that can persist across reboots, allowing users to avoid the workarounds previously required for consistent interface identification. The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer) allows network management data to be more effectively utilized. See the following document for further information: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5ifidx.htm>

NAT - Enhanced H.225/H.245 Forwarding Engine

During the call setup between H.323 terminals, H.225/H.245 protocols are used. The protocol messages contain embedded IP addresses and ports. If a message passes through a NAT router, it has to be decoded, translated and encoded back to the packet. This enhancement extends support to all messages in H.225/H.245 protocols and all embedded addresses.

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 user's 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.

NAT - Support of H.323 v2 Call Signalling (FastConnect)

Cisco IOS Network Address Translation (NAT) supports all H.225 and H.245 message types, including Fast Connect and Alerting as part of H.323 v2. Any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration.

NAT - Support of IP Phone to Cisco Call Manager

Cisco IP Phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco Call Manager (CCM). Messages flow back and forth that include IP address and Port information which is used to identify other IP Phone users with which a call can be placed.

To be able to deploy Cisco IOS Network Address Translation (NAT) between the IP Phone and CCM in a scalable environment, NAT needs to be able to detect the Selsius Skinny Station Protocol and understand the information passed within the messages.

When an IP Phone attempts to connect to the CCM and it matches the configured NAT translation rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address is what will be reflected in the CCM and be visible to other IP Phone users.

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 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 configuration 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.

PIM Dense Mode State Refresh

The PIM Dense Mode State Refresh feature keeps the pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree.

Router-Port Group Management Protocol

The Router-Port Group Management Protocol (RGMP) feature introduces a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic.

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.

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

The following new software features are supported by the Cisco 2500 series routers for Release 12.1(3)T:

Circuit Interface Identification MIB

The Circuit Interface Description MIB feature adds support for a new Cisco enterprise MIB, used for monitoring individual circuits using SNMP. The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object which can be used to provide a description of individual circuit-based interfaces (for example, interfaces using ATM or Frame-Relay). This description will then be returned when linkup and linkdown SNMP traps are generated for the described interface.

The Circuit Interface MIB consists of a single table, with each row being a sequence of two objects: Circuit Interface Description (cciDescr) and Circuit Interface Status (cciStatus).

The cciDescr object is used to identify circuits using a textual description of up to 255 characters specified by the user (note that MIB objects are modified using network management system (NMS) applications, and can not be configured using the Cisco IOS command-line interface). When the row is created by a user, a value is set for the cciDescr object. The table is indexed by ifIndex from the IF-MIB. The cciStatus is the RowStatus object for the rows in the table.

The cciStatus object can be set to only two values by the user: createAndGo(4), which creates a new row, and destroy(6), which removes an existing row. If the row is created successfully, the cciStatus will be active(1). When creating a new row, the user should set the cciDescr object along with the cciStatus in a single **snmp set pdu** command. If the row is already active, only the cciDescr object can be modified. The other option is to delete the row first by setting the cciStatus to destroy(6) and then recreate the row with a new value for cciDescr. When creating a new row, the ifIndex is validated first. If the ifIndex value is not valid, the row is not created and an error code is returned. Similarly, if, when an interface is deleted, there was a corresponding row in this table, that row will be deleted automatically.

After a description is created for an interface, the description (the cciDescr object) will be sent along with the other varbinds as part of linkup and linkdown trap notifications.

Event MIB

The Event MIB is an asynchronous notification mechanism standardized for use by network management systems using Simple Network Management Protocol (SNMP). The Event MIB provides the ability to monitor Management Information Base (MIB) objects on a local or remote system using SNMP and initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified). By allowing notifications based on events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed.

When combined with the Expression MIB support introduced in Cisco IOS Release 12.0(5)T, Event MIB support in Cisco IOS software provides a flexible and efficient way to monitor complex conditions on network devices.

Frame Relay ELMI Address Registration

The Frame Relay ELMI Address Registration feature enables a network management system (NMS) to detect connectivity among the switches and routers in a network using the Enhanced Local Management Interface (ELMI) protocol. During ELMI version negotiation, neighboring devices exchange their management IP addresses and ifIndex. The NMS polls the devices to collect this connectivity information.

Before this feature was introduced, NMS could detect only the topology of routers or the topology of switches. The NMS could not detect router and switch interconnection and was therefore unable to create a complete topology of the network. With the Frame Relay ELMI Address Registration feature, the NMS can detect switch and router interconnection and create an end-to-end network topology map for network administrators.

The Cisco Frame Relay MIB has been enhanced to support the new ELMI information. The NMS uses the MIB to extract the IP address and ifIndex of devices neighboring the managed device.



Note

The ELMI address registration mechanism does not check for duplicate or illegal addresses.

ELMI address registration takes place on all interfaces on which ELMI is enabled, even if all the interfaces are connected to the same router or switch. The router periodically sends a version inquiry message with version information, the management IP address, and ifIndex to the switch. The switch sends its management IP address and ifIndex using the version status message. When the management IP address of the switch changes, an asynchronous ELMI version status message is sent to the neighboring device immediately.

When ELMI is enabled, the router automatically chooses the IP address of one of the interfaces to use for ELMI address registration purposes. The router will choose the IP address of an Ethernet interface first, and then serial and other interfaces. You have the option to use the IP address chosen by the router or to disable the autoaddress mechanism and configure the management IP address yourself. You can also choose to disable ELMI address registration on a specific interface or on all interfaces.

Individual SNMP Trap Support

The Individual SNMP Trap Support Feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are *authentication-failure*, *linkup*, *linkdown*, and *coldstart*. This feature expands the functionality of the **snmp-server enable traps snmp** command. Prior to the introduction of this feature, all four trap types were enabled or disabled simultaneously by the **snmp-server enable traps snmp** command.

Individual SNMP Trap Support is supported for all versions of SNMP supported by Cisco IOS software (SNMPv1, SNMPv2c, and SNMPv3).



Note

As both SNMP traps and informs are enabled or disabled through the use of the **snmp-server enable traps** command, all references to traps in this document also apply to informs. The term "notifications" is used to refer to both traps and informs.

Source Specific Multicast

The Source Specific Multicast feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

Source specific multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast lite suite of solutions targeted for audio and video broadcast application environments.

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

The following new software features are supported by the Cisco 2500 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/BE CN) bits in switched packets when there is network congestion.

Gatekeeper to Gatekeeper Redundancy and Load-Sharing

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism feature expands the capability that is provided by the Redundant H.323 Zone Support feature. With the Redundant H.323 Zone Support feature, the LRQs are sent simultaneously (in a “blast” fashion) to all of the gatekeepers in the list. The gateway registers with the gatekeeper that responds first. Then, if that gatekeeper becomes unavailable, the gateway registers with another gatekeeper from the list.

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism feature enhances this capability by allowing the user to choose whether the LRQs are sent simultaneously or sequentially (one-at-a-time) to the remote gatekeepers in the list. If the LRQs are sent sequentially, a delay is inserted after the first LRQ and before the next LRQ is sent. This delay allows the first gatekeeper to respond before the LRQ is sent to the next gatekeeper. The order in which LRQs are sent to the gatekeepers is based on the order in which the gatekeepers are listed (using either the **zone prefix** or the **gw-type-prefix** command).

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.

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

The following new software features are supported by the Cisco 2500 series routers for Release 12.1(1)T:

Express Resource Transport Protocol and TCP Header Compression (CRTP)

As of Cisco IOS Release 12.0(7)T, if TCP or RTP header compression is enabled, it occurs by default in the fast-switched path or the Cisco Express Forwarding-switched (CEF-switched) path, depending on which switching method is enabled on the interface. Furthermore, the number of TCP and RTP header compression connections is increased to 1000 connections each.

Prior to this feature, such compression was performed in the process-switching path. That meant that packets traversing interfaces that had TCP or RTP header compression enabled were queued and passed up to the process to be switched. This procedure slowed down transmission of the packet, and therefore, some users preferred to fast switch uncompressed TCP and RTP packets.

Pragmatic General Multicast (PGM)

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for multicast applications that require reliable, ordered, duplicate-free multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. PGM has two main parts: a host element (also referred to as the transport layer of the PGM protocol) and a network element (also referred to as the network layer of the PGM protocol).

The transport layer of the PGM protocol consists of two main parts: a source part and a receiver part. The transport layer defines how multicast applications send and receive reliable, ordered, duplicate-free multicast data from multiple sources to multiple receivers. The PGM Host feature is the Cisco implementation of the transport layer of the PGM protocol.

Service Assurance Agent Enhancements

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a mainframe host) by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss and application performance. This feature enables you to perform troubleshooting, problem analysis, and notifications based on the statistics collected by the SA Agent.

The SA Agent Enhancements feature introduces new performance measurement operations and enhancements to assist in the measurement of SLAs. With Cisco IOS Release 12.1(1)T, the SA Agent provides new capabilities that enable you to do the following:

- Measure FTP file download response time using the new FTP operation.
- Monitor one-way latency reporting through enhancements to the Jitter operation.
- Configure a new option for the DHCP operation.
- Manually enable a responder port.
- Verify data for the UDPEcho operation.
- Configure new options for the **rtr schedule** command.
- Restart an operation.

State-Refresh

The **state-refresh** command prevents the periodic timeout of prune state in routers, greatly reducing the reflooding of multicast traffic down the pruned branches that expire periodically. It also causes topology changes to be realized quicker than the traditional three-minute timeout.

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 6.

Table 6 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	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

Table 6 *Deprecated and Replacement MIBs (continued)*

Deprecated MIB	Replacement
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 2500 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> .

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(2)T

This section describes possibly unexpected behavior by Release 12.1(2)T, specific to the Cisco 2500 series routers. Only severity 1 and 2 caveats are included.

CSCdr36952

A defect in Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to “<http://<router-ip>/%%>” is attempted. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS Releases 11.1 through 12.1, inclusive. The vulnerability has been corrected, and Cisco is making fixed releases available 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.

The vulnerability can be mitigated by disabling the IOS HTTP server, using an access-list on an interface in the path to the router to prevent unauthorized network connections to the HTTP server, or applying an access-class option directly to the HTTP server itself. The IOS HTTP server is enabled by default only on Cisco 1003, 1004, and 1005 routers that are not configured. In all other cases, the IOS http server must be explicitly enabled in order to exploit this defect.

The complete advisory, including software fixes and workarounds, is available at:

<http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml> .

Related Documentation

The following sections describe the documentation available for the Cisco 2500 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 23
- Platform-Specific Documents, page 24
- Feature Modules, page 24
- Cisco IOS Software Documentation Set, page 25

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

These individual and groups of documents are available for the Cisco 2500 series routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 2524 and Cisco 2525 Public Network Certification*
- *Installing WAN Modules in the Cisco 2524 and Cisco 2525 Routers*
- *Cisco 2524 and Cisco 2525 Router User Guide*
- Release notes for Cisco 2500 series routers
- *Redundant Power Systems*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

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 7 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 7 Cisco IOS Software Release 12.1 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	<ul style="list-style-type: none"> Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	<ul style="list-style-type: none"> Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	<ul style="list-style-type: none"> IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	<ul style="list-style-type: none"> AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband

Table 7 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	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
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> • <i>New Features in 12.1-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.1 T</i> • Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms) • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> 	

**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 23.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQuick Study, iQ Readiness Scorecard, The iQ Logo, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document/website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0008R)

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

