



# Release Notes for Cisco AS5300 Universal Access Servers for Cisco IOS Release 12.1 T

---

May 8, 2001



**Note**

---

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

---

These release notes for the Cisco AS5300 universal access servers describe the enhancements provided in Cisco IOS Release 12.1(5)T. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.1(5)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 Connection Online (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:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 9
- Limitations and Restrictions, page 24
- Important Notes, page 26
- Caveats, page 28
- Related Documentation, page 28
- Obtaining Documentation, page 33
- Obtaining Technical Assistance, page 34



---

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

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

78-10638-04 Rev. B0

# Introduction

The Cisco AS5300 is a versatile data communications platform that performs two functions in a single modular chassis depending on the installed feature cards and IOS images:

- Remote Access Server
- Voice Gateway

The remote access server is intended for Internet service providers (ISPs), telecommunications carriers, and other service providers that offer managed Internet connections and medium to large sites that provide both digital and analog access to users on an enterprise network. By terminating both analog and digital calls on the same chassis simultaneously, the access server provides a clear, simple, and easy migration path from analog dial access services to digital dial access services.

The Cisco AS5300/Voice Gateway is a versatile data communications platform that provides the functions of an access server, router, and digital modem(s) in a single modular chassis. The Cisco AS5300 includes three feature card slots: one holds a T1/E1/PRI feature card, and the other two support modem feature cards or voice digital signal processor (DSP) feature cards. When equipped with modem cards, the Cisco AS5300 serves as a remote access concentrator for dial-up (modem or ISDN) Internet access. When equipped with voice feature cards and Voice IOS, the Cisco AS5300/Voice Gateway serves as a voice (VoIP) gateway. By using one slot for modems and the other for voice DSPs, the Cisco AS5300 can serve in both capacities. Modem, voice, or fax calls are routed to the appropriate cards/resources via Dialed Number Identification Service (DNIS).

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.1(5)T, see the “New and Changed Information” section on page 9 and the “Related Documentation” section on page 28.

## System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(5)T:

- Memory Recommendations, page 3
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Microcode and Modem Code Software, page 4
- Feature Set Tables, page 5

## Memory Recommendations

Memory recommendations for the Cisco AS5300 are presented in Table 1.

**Table 1** *Memory Recommendations for the Cisco AS5300*

Feature Set	Image Name	Flash Memory Recommended	DRAM Memory Recommended	Runs From
IP	c5300-i-mz	16 MB	64 MB	RAM
IP Plus	c5300-is-mz	16 MB	64 MB	RAM
IP Plus IPsec 56	c5300-is56i-mz	16 MB	64 MB	RAM
IP Plus IPsec 3DES	c5300-ik2s-mz	16 MB	64 MB	RAM
IP/IPX/AT/DEC	c5300-d-mz	16 MB	64 MB	RAM
IP/IPX/AT/DEC Plus	c5300-ds-mz	16 MB	64 MB	RAM
Enterprise	c5300-j-mz	16 MB	64 MB	RAM
Enterprise Plus	c5300-js-mz	16 MB	64 MB	RAM
Enterprise Plus IPsec 56	c5300-js56i-mz	16 MB	64 MB	RAM
Enterprise Plus IPsec 3DES	c5300-jk2s-mz	16 MB	64 MB	RAM

## Hardware Supported

Cisco IOS Release 12.1(5)T supports the Cisco AS5300. The supported interfaces are detailed in Table 2.

For detailed descriptions of the new hardware features, see “New and Changed Information” section on page 9.

**Table 2** *Supported Interfaces for the Cisco AS5300*

Interface and Modem Cards	Product Description
Interface Cards	Ethernet RJ-45 (included with unit)
	Ethernet/Fast Ethernet (RJ-45) (included with unit)
	ISDN PRI
	E1-G.703/G.704
	Channelized T1 (4 ports) without serial support
	Channelized T1 (4 ports) with 4 serial ports
	Channelized T1 (8 ports) with 4 serial ports
	Channelized E1 (4 ports) without serial support
	Channelized E1 (4 ports) with 4 serial ports
	Channelized E1 (8 ports) with 4 serial ports

**Table 2** Supported Interfaces for the Cisco AS5300 (continued)

Interface and Modem Cards	Product Description
Interface Cards (continued)	HMM/48 channel
	HMM/54 channel
	HMM/60 channel
	DMM/48 channel
	DMM/96 channel
	DMM/108 channel
	DMM/120 channel
	48-Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)
	60-Channel, TI C549-based VoIP feature card (Uses High Density AS53-VOXD DSP modules)
	24-Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)
48-Channel, TI C542-based VoIP feature card (First generation, uses AS53-6VOX DSP modules)	
Interface Cards	MICA modems
	Microcom 56K modems

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5300, log in to the Cisco AS5300 and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software c5300-i-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 *Cisco IOS Upgrade Ordering Instructions* located at:

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm)

## Microcode and Modem Code Software

Microcode software images are bundled with the system software image—with the exception of the Channel Interface Processor (CIP) microcode (all system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. Table 3 lists the current microcode versions for the Cisco AS5300.

You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

The modem code release notes are on Cisco.com and the Documentation CD-ROM:

On Cisco.com at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Firmware and Portware Information**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Firmware and Portware Information**

**Table 3** *Current Modem Code Versions for the Cisco AS5300*

Modem Module	Current Bundled Modem Code Version	Minimum Cisco IOS Release Required
Microcom modems	Microcom Version 5.1.20	12.0(5)T and later
MICA modems	MICA portware Version 2.7.1.0	12.0(5)T and later

## Feature Set Tables

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



### Caution

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

Table 4 lists the features and feature sets supported by the Cisco AS5300 in Cisco IOS Release 12.1(5)T and uses the following conventions:

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



### Note

This table might not be cumulative or list all the features in each image. 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. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.1(5)T by using the Feature Navigator tool at: <http://www.cisco.com/go/fn>.

Table 4 Feature List by Feature Set for the Cisco AS5300

Feature	In <sup>1</sup>	Software Images by Feature Set									
		IP	IP Plus	IP Plus IPsec 56	IP Plus IPsec 3DES	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES
<b>New Features in 12.1(5)T</b>											
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Calling Line Identification Screening—Call Discriminator	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deutsche Telekom Phase I	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dial Modifiers	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer DNIS-Group Range	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
ISDN Progress Indicator support for SIP using 183 Session Progress	(5)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
L2TP Tunnel Management Enhancements	(5)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Monitoring Resource Availability on Cisco AS5x00 Universal Access Servers	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Radius Tunnel Attribute Extensions	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Sticky IP	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
T.37/T.38 Fax Gateway	(5)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
VoIP Call Admission Control using RSVP	(5)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco AS5300 (continued)

Feature	In <sup>1</sup>	Software Images by Feature Set									
		IP	IP Plus	IP Plus IPsec 56	IP Plus IPsec 3DES	Desk-top	Desk-top Plus	Enter-prise	Enter-prise Plus	Enter-prise Plus IPsec 56	Enter-prise Plus IPsec 3DES
<b>New Features in 12.1(3a)T1</b>											
AAA Session MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco AAA Server MIB and Additional Enhancements for the Cisco AS5300 and Cisco AS5800	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fax Relay Packet Loss Concealment	(3)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interactive Voice Response Version 2.0 on Cisco VoIP Gateways	(3)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Media Gateway Control Protocol Residential Gateway Support	(3)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Monitoring Resource Availability on Cisco AS5300 Universal Access Servers	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Preauthentication with ISDN PRI and Channel-Associated Signaling	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Internet</b>											
<b>IP Routing</b>											
H.323 Version 2 Support		No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Asynchronous Serial Traffic over UDP		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>LAN Support</b>											
Subnetwork Bandwidth Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLI String Search		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encaps for Dial-in over ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN LAPB-TA		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Dialout		No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
OS_IFSS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco AS5300 (continued)

Feature	In <sup>1</sup>	Software Images by Feature Set									
		IP	IP Plus	IP Plus IPsec 56	IP Plus IPsec 3DES	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES
SS7		No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
<b>Management</b>											
CNS Client for Cisco IOS Software		No	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes
CNS client for IOS 12.05(t) (aka IPsec Policy Agent II)		No	No	No	No	No	No	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Routing Monitor		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists Using Time Ranges		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>											
Cisco IOS DHCP Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Store-and-Forward Fax		No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
IPX Infrastructure Enhancements		No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Personal Handyphone Internet Access Forum Standard (PIAFS) <sup>2</sup>	(2)	No	Yes	Yes	Yes	No	No	No	No	No	No
TDM Hairpinning		No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Voice over IP Q.SIG Network Transparency for Cisco AS5300		No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
<b>Quality of Service</b>											
Parse Bookmarks		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security</b>											
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AAA Server Group Enhancements	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Preauthentication with ISDN PRI	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resource Pool Management		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resource Pool Management with Direct Remote Services		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Console		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Switching</b>											
Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway	(1)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco AS5300 (continued)**

Feature	In <sup>1</sup>	Software Images by Feature Set									
		IP	IP Plus	IP Plus IPsec 56	IP Plus IPsec 3DES	Desk-top	Desk-top Plus	Enterprise	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES
<b>Voice Technologies</b>											
Configurable Timers in H.225	(2)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	(2)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Inband MICA Control Message for PPP Framing	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PRI/Q.931 Signaling Backhaul for Call Agent Applications	(1)	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes

1. The number in the "In" column indicates the Cisco IOS release when the interface was introduced. For example, (1) means an interface was introduced in Cisco IOS Release 12.1(1)T. If a cell in this column is empty, the interface was included in the initial base release.
2. PIAFS is an error-correcting link layer protocol used in Japan over PHS digital server networks. PIAFS Version 2.0 requires Cisco IOS Software Release 12.1(2a)XH or higher and is supported on Cisco AS5300 and Cisco AS5800 universal access servers. Contact your account representative for information about obtaining Cisco MICA portware for PIAFS.

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5300 for Cisco IOS Release 12.1(5)T.

### New Hardware Features in Cisco IOS Release 12.1(5)T

There are no new hardware feature in the Cisco AS5300 for 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 AS5300 for Cisco IOS Release 12.1(5)T.

#### AutoInstall Using DHCP for LAN Interfaces (CSCdr88175)

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 that 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. Before 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 Trivial File Transfer Protocol (TFTP).

For further details, please see:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt\\_dhcpa.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_dhcpa.htm)

## Dial-on-Demand Authentication Enhancements (CSCdp96375)

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 vendor-specific attribute (VSA), “outbound:send-name=<string>”.

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

## 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 can 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 (SSM) 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 SSM: URL Rendezvous Directory (URD) and IGMP v3lite. Both of these features were introduced with SSM in Cisco IOS Release 12.1(5)T.

## Interface Index Persistence

One of the most commonly used identifiers 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 Requests for Comments (RFC) 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, enabling 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) enables network management data to be used more effectively. See the following document for further information: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5ifidx.htm>.

## Interface Range Specification

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range. The Interface Range Specification feature is implemented with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the **range** keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

## Interworking Signaling Enhancements for H.323 and SIP VoIP

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables Voice over IP (VoIP) networks to properly signal the setup and tear-down of calls when interworking with Public Switched Telephone Networks (PSTNs). These enhancements ensure that in-band tones and announcements are generated when needed so that the voice path is cut-through at the appropriate point of call setup and that early alerting (ringing) does not occur. In addition, support for network-side ISDN and the reducing of speech clipping is addressed.

## Monitoring Resource Availability on Cisco AS5300, AS5400, and AS5800 Universal Access Servers

This feature provides enhancements to improve the visibility into the line and modem status for the network access server (NAS).

NAS modem health is supported by the following features:

- DS-0 Busyout Traps
- ISDN PRI Requested Channel Not Available Traps
- Modem Health Traps
- Show Controllers Timeslots
- DS-1 Loopback Traps

These features have been developed to monitor the NAS health conditions at the digital signal level zero (DS-0) level, Primary Rate Interface (PRI) bearer channel level, and modem level.

This combined set of features provides the following benefits:

- Improved visibility into the line status for the NAS for comprehensive health monitoring and notification capability.
- Improved troubleshooting and diagnostics for large dial networks.

## NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)

Microsoft NetMeeting is a Windows-based application that enables multiuser 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.

## 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 control lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines that 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 reenabling 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.

## Preauthentication Enhancements for Callback

The Preauthentication Enhancements for Callback feature allows users to dial into the NAS without being charged. This enables telecommuters, and other remote network users who dial in, to have the charges applied back to the NAS into which they are dialing.

Two Cisco VSAs for preauthentication will be added to Attribute 26 as follows:

```
cisco-avpair = "preauth:send-name=<string>"
cisco-avpair = "preauth:send-secret=<string>"
```

## Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements (CSCdp96375)

This feature supports the use of new RADIUS VSAs. These RADIUS VSAs are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used. Enhancements for this feature include:

- Attribute 6 can be set to Service-Type = Framed-User
- Support for new VSAs "preauth:send-name" with text and "preauth:send-secret" with text.

## RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements (CSCdp96375)

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature enables the user to specify the hostname of the NAS in attribute 66, rather than the IP address. This feature frees the user from having to remember the numerical IP address of the NAS, and may also provide a small measure of security by protecting the numerical IP address of the NAS.

## RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

## RADIUS Tunnel Attribute Extensions

The RADIUS Tunnel Attribute Extensions feature introduces RADIUS attribute 90 (Tunnel-Client-Auth-ID) and RADIUS attribute 91 (Tunnel-Server-Auth-ID). Both attributes help support the provision of compulsory tunneling in virtual private networks (VPNs) by allowing the user to specify authentication names for the network access server (NAS) and the RADIUS server.

Once a NAS has set up communication with a RADIUS sever, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. Attributes 90 and 91 support Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP).

Attributes 90 and 91 must be included if the RADIUS sever accepts the request and the desired authentication name is different from the default.

Attributes 90 and 91 should be included in an accounting request that contains Acct-Status-Type attributes with values of either start or stop and that pertains to a tunneled session.

## Router-Port Group Management Protocol (CSCdp11190)

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 Synchronous Data Link Control (SDLC) configurations, and a new timeout setting for the Set Normal Response (SNRM) frame. These enhancements change the operation of SDLC processing on a multidrop line.

## Window Size Setting

Before this feature, all SDLC addresses on the multidrop had the same window count. Now the window count can be configured on a Physical Unit 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 uses 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 use 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.

## T.37/T.38 Fax Gateway

Previously, Store and Forward Fax was supported only on modem cards while voice applications ran on the C542 Digital Signal Processing Module (DSPM) and C549 DSPMs that populated Cisco AS5300 Voice Feature Cards (VFCs). Each type of call required different technologies. With this software release, a single DSPM technology will support:

- Voice, fax relay, and Store and Forward Fax on both the C542 and C549 DSPM and the same voice port.
- Dynamic switching from one application to another in the same call (IVR, voice, fax relay, and Store and Forward Fax).

When the Cisco AS5300 is equipped with VFCs, it supports carrier-class VoIP and fax over IP services. Since the Cisco AS5300 is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and voice activity detection (VAD)/silence suppression. There is an interactive voice response (IVR) application that provides voice prompts and digit collection in order to authenticate the user and identify the call destination.

The VFC is a coprocessor card with a powerful reduced instructions set computing (RISC) engine and dedicated, high-performance Digital Signal Processors (DSPs) to ensure predictable, real-time voice processing. The design enables steamlined packet forwarding. The Cisco AS5300 supports two VFCs, which are scalable up to 96 E1 or 120 T1 voice connections within a single chassis.

## UDLR Tunnels 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 (UDLR) 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 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 RSVP feature synchronizes Resource Reservation Protocol (RSVP) procedures with H.323 Version 2 (Fast Connect) setup procedures to guarantee that the required Quality of Service (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 Hardware Features in Cisco IOS Release 12.1(3a)T1

There are no new hardware feature in the Cisco AS5300 for Cisco IOS Release 12.1(3a)T1.

## New Software Features in Cisco IOS Release 12.1(3a)T1

The following new software features are supported by the Cisco AS5300 for Cisco IOS Release 12.1(3a)T1.

### AAA Session MIB

Customers are demanding the ability to both monitor and terminate their authenticated client connections via SNMP. Furthermore, customers are requesting that the client data provided be directly related to the accounting information reported by AAA to either Radius or Tacacs. Moreover, additional real-time information such as idle times are also requested for this feature in order to provide the ability to terminate calls with no activity present.

This feature allows Cisco's customers to extend and expand their ability to monitor end users by providing access to some client data objects via SNMP.

### Circuit Interface Identification MIB

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

For further details, see the CISCO-CIRCUIT-INTERFACE-MIB.my file, available from the Cisco Connection Online MIB site at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## Cisco AAA Server MIB and Additional Enhancements for the Cisco AS5300 and Cisco AS5800

### Addition to show caller Command

The **show caller** command combines the output of the existing call-related show commands. This command displays connection status in summary or in detail. The summary field has been added (summary) to display the total number of calls, including the number of ISDN and Analog calls, since the last reload. This summary counter is cumulative of all calls since the NAS has been up, where other counters indicate the current number of calls in the NAS.

Using the **show caller** command provides the following benefits:

- Displays statistics or debug information for connections using a single command
- Replaces the need to know and use the various show commands
- Provides network management across all Cisco platforms

### Cisco AAA Server MIB

This MIB provides statistics reflecting the state of AAA Server operation within the device and AAA communications with external servers.

The Cisco AAA Server MIB provides the following information:

- Distinct statistics for each AAA function
- Status of servers providing AAA functions
- Identities of external AAA servers

A server is defined as a logical entity that provides any of the three AAA functions. A TACACS+ server consists of all three functions with a single IP address and single TCP port. A RADIUS server can consist of the authentication/accounting pair with a single IP address but distinct UDP ports, or it may be just one of authentication or accounting.

### Point-to-Point Password Authentication Protocol Refusal

This new command allows refusal of a peer's request to remote (Point-to-Point Protocol [PPP]) authenticate using Password Authentication Protocol (PAP).

### 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. 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.

Support of the Event MIB has been added to Cisco IOS software to work with a variety of network management systems and, when combined with the currently integrated Expression MIB support, provides a flexible and efficient way to monitor complex conditions on network devices. By allowing SNMP notifications to take place only when a specified condition occurs, Event MIB support reduces the load on affected devices, significantly improving the scalability of network management solutions.

For documentation, see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtevent.htm>

## Fax Relay Packet Loss Concealment

This feature improves the current real-time fax over IP (commonly known as fax relay) implementation in Cisco gateways, allowing fax transmissions to work reliably over higher packet loss conditions.

In addition, this feature includes enhanced real-time fax debug capabilities and statistics. These debugs and statistics will 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 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).

## 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”, “linkup”, “linkdown”, and “coldstart”. This feature expands the functionality of the **snmp-server enable traps snmp** command.

For documentation, see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtitraps.htm>

## Interactive Voice Response Version 2.0 on Cisco VoIP Gateways

IVR Version 2.0 is the fourth release of IVR and TCL scripting on Cisco IOS VoIP gateways. The Cisco IVR feature (first made available in Cisco IOS Release 12.0(3)T and 12.0(7)T) provides IVR capabilities using TCL scripts.

IVR Version 2.0 is made up of several separate components which are described individually in the section that follows. These new features include:

- Media Gateway Control Protocol (MGCP) scripting package implementation
- Real Time Streaming Protocol (RTSP) client implementation
- New Tool Command Language (TCL) verbs to utilize RTSP and MGCP scripting features
- IVR prompt playout and digit collection on IP call legs
- Performance improvements and TCL infrastructure changes
- IVR application MIB for network management

These features add scalability and enable the IVR scripting functionality on VoIP legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers.

## Media Gateway Control Protocol Residential Gateway Support

MGCP Residential Gateway Support (RGW) merges the Simple Gateway Control Protocol (SGCP) 1.1 with the Media Gateway Control Protocol (MGCP) 0.1. The protocols describe the types of calls a network gateway can accept and what it does with the calls it receives. The merged set enables a single gateway to receive commands from either protocol.

A network gateway handles the translation between audio signals and the packet network. The gateway interacts with a Call Agent, which performs signal and call processing on the gateway's calls. MGCP RGW supports both Residential Gateways and Trunking Gateways.

A Residential Gateway (RGW) provides the interface between analog calls from a telephone or PBX and the Voice over IP network. The Cisco uBR924 and 2600 platforms are RGWs. Additional features supported on both RGWs are call waiting, stutter dialtone, and modem and fax calls. The uBR924 platform also supports onhook caller ID, distinctive ringing, and ring splash.

A Trunking Gateway (TGW) provides the interface between Public Switched Telephone Network (PSTN) trunks and the Voice over IP network. The Cisco AS5300 and 3660 platforms are TGWs. Additional features supported on both TGWs are SS7, modem, and fax calls, and T1 interfaces. The AS5300 also supports 911 outgoing calls on T1 lines, PRI/ISDN signaling, and E1 interfaces.

## Monitoring Resource Availability on Cisco AS5300 Universal Access Servers

This set of features provides enhancements to improve visibility into the line and modem status for the network access server (NAS). The combined features in this document have been developed to monitor the NAS health conditions at the DS0 level, PRI bearer channel level, and modem level.

These features are enabled and disabled by enhanced command-line interface and MIBs.

NAS modem health monitoring is supported by the following features:

- DS0 Busyout Traps
- PRI Requested Channel Not Available Traps
- Modem Health Traps
- Controller Time Slots State

## Preauthentication with ISDN PRI and Channel-Associated Signaling

The Preauthentication with ISDN PRI and Channel-Associated Signaling feature allows a Cisco network access server (NAS) to determine if an incoming call may be answered on the basis of the called number, the calling number, or the call type. With an ISDN PRI (Primary Rate Interface), or with Channel-Associated Signaling (CAS), information about an incoming call is available to the NAS before the call is answered. The available call information includes the called station ID (DNIS), the calling station ID (CLID), and the bearer capability (call type).

When an incoming call arrives from the public network switch, but before it is answered, this feature enables the NAS to send the DNIS, CLID, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then the NAS sends a disconnect message to the public network switch to reject the call. This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication based on the CLID at the same time.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

In the event that the RADIUS server application becomes unavailable, this feature allows a guard timer to be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without the authorization.

## New Hardware Features in Cisco IOS Release 12.1(2) T

There are no new hardware feature in the Cisco AS5300 for Cisco IOS Release 12.1(2)T.

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

The following new software features are supported by the Cisco AS5300 for Cisco IOS Release 12.1(2)T:

### AAA Server Group Deadtimer (CSCdp13160)

The AAA Server Group Deadtimer feature allows each authentication, authorization, and accounting (AAA) server to be fully configured in the server group. Thus, it allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

With the introduction of this feature, deadtimer has been added as a new attribute to the server group structure. In addition, a separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and time-outs, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

### Configurable Timers in H.225 (CSCdp30190)

The Configurable Timers in H.225 feature allows users to configure the H.225 TCP connection timeout value for all outgoing call attempts (on a per VoIP dial-peer basis).

In previous releases of the Cisco IOS software, the call attempt timeout was 15 seconds and could not be changed. In some cases, however, users might need a shorter timeout value to facilitate a faster fail-over. In other cases, users might need a greater timeout value.

The Configurable Timers in H.225 feature addresses those needs by allowing the user to override the default of 15 seconds and configure the timeout value.

## Ecosystem Gatekeeper Interoperability Enhancements, Phase 2 (CSCdp70719)

The Ecosystem Gatekeeper Interoperability Enhancements, Phase 2 feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection (ARJ). This allows a gateway to move between gatekeepers during the admission request (ARQ) phase.

## H.323 Support for Virtual Interfaces

The H.323 Support for Virtual Interfaces feature allows users to configure the IP address of the gateway, so that the IP address included in the H.323 packet is deterministic and consistently indicates the same address for the source.

In previous releases of the Cisco IOS software, the source address included in the H.323 packet could vary depending on the protocol (RAS, H.225, H.245, or RTP). This makes it difficult to configure firewall applications to work with H.323 messages.

The H.323 Support for Virtual Interfaces feature addresses that difficulty by allowing the user to explicitly configure an IP address to be used for all protocols.

## Inband MICA Control Messages for PPP Framing (CSCdk36386 and CSCdp88103)

Dialin internet connections typically start in character mode to let the general user log in and select a preferred service. When Cisco IOS determines that the user wants a framed interface protocol during the call, such as PPP or SLIP, commands are sent to the MICA modem so it will provide hardware assistance with the framing. To avoid loss or misinterpretation of framed data during the transition, these commands must be issued at precise times with respect to the data being sent and received. The Inband MICA Control Messages for PPP Framing feature allows the MICA modem framing commands to be sent in the data stream itself, which greatly simplifies Cisco IOS's tasks in achieving precision timing, and reduces timeouts during PPP startup and also reduces startup time.

## OSPF Flooding Reduction (CSCdp80470)

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 sec. Some implementations have tried to improve the flooding by reducing the frequency to refresh from approximately 30 to 50 minutes. 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 Do Not Age (DNA) LSAs.

All OSPF customers with generally stable networks will benefit from the reduced traffic overhead provided by the OSPF Flooding Reduction feature.

## Preauthentication with ISDN PRI (CSCdm82434)

The Preauthentication with ISDN PRI feature allows a Cisco network access server (NAS) to determine if an incoming call may be answered on the basis of the called number, the calling number, or the call type. With an ISDN PRI (Primary Rate Interface), information about an incoming call is available to the NAS before the call is answered. The available call information includes the called station ID (DNIS), the calling station ID (CLID), and the bearer capability (call type).

When an incoming call arrives from the public network switch, but before it is answered, this feature enables the NAS to send the DNIS, CLID, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then the NAS sends a disconnect message to the public network switch to reject the call. This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication based on the CLID at the same time.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

In the event that the RADIUS server application becomes unavailable, this feature allows a guard timer to be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call without the authorization.

## New Hardware Features in Cisco IOS Release 12.1(1) T

There are no new hardware features in the Cisco AS5300 for Cisco IOS Release 12.1(1) T.

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

The following new software features are supported by the Cisco AS5300 for Cisco IOS Release 12.1(1) T:

### AAA DNIS Map for Authorization

The AAA DNIS Map for Authorization feature allows you to select AAA server groups—to which authorization requests can now be sent—using DNIS. This feature is an enhancement to Selecting AAA Server Groups Based on DNIS, Cisco IOS Release 12.0(7)T, which allows you to send authentication and accounting requests when selecting a AAA server group using DNIS.

With the introduction of this feature, authorization requests are available so that you can specify the same server group for AAA services or a separate server group for each AAA service. Thus, you can configure authorization on different physical devices and provide fail-over backup support.

## Cisco H.323 Version 2 Phase 2

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding several optional features of the H.323 Version 2 specification and facilitates 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 that must be done 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 standalone 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).

- 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).

- 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.

## Dial Peer Enhancements

The Dial Peer Enhancements to the dial peer configuration limit complexity of dial planning and reduce the amount of effort in creating dial peer entries. These include additional dial string symbols, translation rule implementation, number translation, and digit stripping option.

## Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway

The Media Gateway Control Protocol (MGCP) for the Cisco AS5300 is a protocol that media gateways use for passing voice calls from the Public Switched Telephone Network (PSTN) to call agents in an internet telephony network. Media gateways include trunking gateways, access gateways, and network access servers. The call agents provide the call control intelligence.

Caveat for 12.1(1)T:

The **show mgcp** command displays the status of mgcp on the system. The display includes a line  
 MGCP simple-sdp DISABLED, MGCP cisco fgdos DISABLED

These two commands are for Cisco use only in Release 12.1(1)T.

## PRI/Q.931 Signaling Backhaul for Call Agent Applications

PRI/Q.931 Signaling Backhaul for Call Agent Applications provides the ability to reliably transport the signaling (Q.931 and above layers) from a PRI trunk that is physically connected to a media gateway (for example, a Cisco AS5300) to a media gateway controller (Cisco VSC3000) for processing.

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. Two new features, Roaming and Multiple Roots have been added in Cisco IOS Release 12.1(1)T to enhance the OSP. The VoIP/Open Settlement Protocol (OSP) feature offers the ability to authorize, route calls, and billings between two different ISPs via a trusted third party, the settlement clearing house, which is the OSP server. Cisco has built this OSP client on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms, and partnered with a few companies (TransNexus, GRIC, etc.) that provide OSP servers.

The code for this feature is an encrypted image.



### Note

Before you can download 56-bit or 56i encryption images, you must first go through the entitlement process. This process makes sure your system is coming from a registered DNS address and that you're not coming from an encryption-restricted country (Iraq, Libya, etc.). You (and your customers) can entitle yourselves by filling out the forms located at the following URL:

<http://www.cisco.com/kobayashi/library/12.0/>

## Session Initiation Protocol Gateway Call Flows

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks.

SIP uses six request methods:

- INVITE—Indicates a user or service is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.

- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server. Gateways do not support the REGISTER method.

The following types of responses are used by SIP and generated by the Cisco SIP gateway:

- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

## Settlement Plus Roaming and PKI Multiple Roots on Cisco Access Platforms (Settlements for Packet Voice, Phase 2)

The Cisco gateway based Settlement protocol interacts between carriers to create a single authentication at initialization. Two new features, Roaming and Multiple Roots have been added in Cisco IOS Release 12.1(1)T to enhance the OSP. The VoIP/Open Settlement Protocol (OSP) feature offers the ability to authorize, route calls, and billings between two different ISPs via a trusted third party, the settlement clearing house, which is the OSP server. Cisco has built this OSP client on Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms, and partnered with a few companies (TransNexus, GRIC, etc.) that provide OSP servers. The code for this feature is an encrypted image.



**Note** Before you can download 56-bit or 56i encryption images, you must first go through the entitlement process. This process makes sure your system is coming from a registered DNS address and that you're not coming from an encryption-restricted country (Iraq, Libya, etc.). You (and your customers) can entitle yourselves by filling out the forms located at the following URL:  
<http://www.cisco.com/kobayashi/library/12.0/>

# 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*

<b>Deprecated MIB</b>	<b>Replacement</b>
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 section contains important notes about Cisco IOS Release 12.1(5)T that can apply to the Cisco AS5300.

### Deferral of AS5300 Boot Image

The c5300-boot-mz image has been deferred in Cisco IOS Release 12.1(5)T because of a severe defect. This defect has been assigned Cisco Caveat ID CSCdu10569. The software solution for this defect is the c5300-boot-mz image in Cisco IOS Release 12.0(4)T1.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

**Caution**

---

Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

---

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

### Caveat CSCds52536

An incorrect notification of the released call for a given channel is given to the resource management (RM). RM was unable to authenticate the call again on the same channel resulting in no call being possible on that channel. There is no workaround.

## Caveat CSCds53722

When a gateway calling card uses a PRI signal, a reload may occur.

This has been resolved in Cisco IOS Release 12.1(5)T.

## Caveat CSCds54057

A Cisco gateway running Cisco IOS Release 12.1(4.4)T2 on phone one using Voice over IP (VoIP) to call another Cisco gateway running Cisco IOS Release 12.0(7)xr2 on phone two can hear voice on phone one, but phone one can still hear ringback with no voice.

This has been resolved in Cisco IOS Release 12.1(5)T.

## Caveat CSCds56049

A Cisco 5300 series universal access server using a Cisco gateway running Voice over IP (VoIP) will disconnect a call from phone one to phone two without sending a “stop-account message” for call leg one.

This has been resolved in Cisco IOS Release 12.1(5)T.

## Caveat CSCds57077

If the balance in a portal account is more than 300RMB the portal billing system will return the number 13 in a second authorization attempt which means a toll free call. Because interactive voice response (IVR) does not support the long pound function for a toll free call the call will be disconnected.

For portal accounts with a balance less than 300RMB the portal billing system will return the number 0 which is the normal setting, but the portal console still shows there is something wrong and IVR script will terminate.

This has been resolved in Cisco IOS Release 12.1(5)T.

## 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.

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.

# 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 12.1, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.1 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>.

## Related Documentation

The following sections describe the documentation available for the Cisco AS5300. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- Release-Specific Documents, page 28
- Platform-Specific Documents, page 29
- Feature Modules, page 30
- Cisco IOS Software Documentation Set, page 30

## 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 T*

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 Cisco IOS 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 documents are available for the Cisco AS5300 on Cisco.com and the Documentation CD-ROM:

- *Cisco AS5300 Universal Access Server Quick Start Guide (with Fast Step)*
- *Cisco AS5300 Universal Access Server Chassis Installation Guide*
- *Cisco AS5300 Universal Access Server Module Installation Guide*
- *Cisco AS5300 Universal Access Server Software Configuration Guide*
- *Configuring Cisco IOS Software Features*
- Cisco IOS Release Notes
- *Dial Case Study*
- Port Information—Firmware/portware release notes, configuration notes, command references, FAQs (frequently asked questions)
- Documentation for Spare Parts—Removal and replacement procedures for modem modules, feature cards, power supply
- *Regulatory Compliance and Safety Information*
- *Release Notes for Cisco MICA Portware Version 8.2.1.1 on Cisco AS5x00 Universal Access Servers*
- *Single and High Density VoIP Support for the Cisco AS5300/Voice Gateway*
- *Media Gateway Control Protocol for the Cisco AS3500 Voice/Gateway*

On Cisco.com at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5300**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300**

## Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1(5)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 if 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**

<b>Books</b>	<b>Major Topics</b>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i></li> </ul>	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling 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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX

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

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>New Features in 12.1-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.1 T</i></li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> </ul>	

**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 latest 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**.

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at [http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml).

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. 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 Connection Online (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 Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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](http://www.cisco.com)
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using Cisco.com to [cco-team@cisco.com](mailto: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](http://www.cisco.com/techsupport).

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

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

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 login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

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

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](mailto: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 28

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

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

Copyright © 2001, Cisco Systems, Inc.  
All rights reserved.