



Text Part Number: 78-6150-04

Release Notes for Cisco AS5800 Universal Access Servers for Cisco IOS Release 12.0 T

December 13, 1999

These release notes for Cisco AS5800 universal access servers support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.0 T, refer to the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release, and is location on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the “Caveats” section on page 24 of these release notes.

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

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 11
- Limitations and Restrictions, page 23
- Important Notes, page 24
- Caveats, page 24
- Service and Support, page 30
- Cisco Connection Online, page 31
- Documentation CD-ROM, page 32

Corporate Headquarters

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

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

Introduction

The Cisco AS5800 is a high-density, Integrated Services Digital Network (ISDN) and modem Wide Area Network (WAN) aggregation system that provides digital and analog call termination. It is intended to be used as a service provider dial point-of-presence (POP) or centralized enterprise dial gateway. The Cisco AS5800 consists of a dial shelf, a router shelf, and (optionally) a system controller:

- The Cisco DS5814 (dial shelf) has 14 slots and can support 1 or 2 dial shelf controller cards and up to 12 feature cards to provide full analog modem and ISDN coverage. The dial shelf supports up to 1440 simultaneous analog and/or digital calls. Analog calls are terminated by a feature card that is loaded with integrated modems. ISDN calls are terminated onboard the trunk card on High-Level Data Link Control (HDLC) controllers. The E1 trunk and the T1 trunk card include channel service units (CSUs) and has either 12 E 1 ports or 12 T1 ports that can operate as Primary Rate Interface (PRI) interfaces or channelized interfaces in any combination. The specific trunk card limitations are 1 CT 3 card or up to four 12-port T 1 or four 12-port E 1 cards.

Note T 1 and E 1 cards are not supported in the same box.

- The Cisco RS7206 (router shelf) contains a network processing engine, an I/O controller, and the egress interfaces, such as High-Speed Serial Interface (HSSI), Fast Ethernet (FE), Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM), and supports either 280W AC-input or 280W DC-input redundant power. The router shelf also may contain one or two dial shelf interconnect port adapters each with a single RJ-45 receptacle, which is used to connect the router shelf to the Cisco 5814 dial shelf. The interconnect port adapter connects directly to the dial shelf controller card on the dial shelf via full-duplex cable. The cable used for this connection is a Cisco-proprietary cable, customized with jack screws to secure the connection. You must use this specially designed cable that ships with your interconnect port adapter.
- The Cisco SC3640 (system controller) includes the Cisco 3640 router running Cisco IOS software. The system controller can be installed at a remote facility so users can access multiple systems through a console port or Web interface. System administrators can download software configurations to any Cisco AS5800 universal access server using Simple Network Management Protocol (SNMP) or Telnet. The system controller monitors Cisco equipment to provide performance data collection, accounting data collection, and logging.

The AC-input power shelf is an optional component of the Cisco AS5800 universal access servers and is used to convert AC-input power into DC-output power for the DC-powered Cisco 5814 dial shelf. The AC-input power shelf contains two AC-input power supplies.

The Cisco AS5800 universal access servers accept AC-input power via a separate, self-contained AC-input power shelf, which converts AC-input power into DC-output for use by the DC-powered dial shelf. The AC-input power shelf is rack-mounted and has a safety cover that shields the electrical connections in the power shelf rear.

The AC-input to DC-output connection supplies -48V DC-output power to the dial shelf power entry modules (PEMs). The PEMs receive the -48 volts and transmit power to the filter module. Power flows through the filter module to the backplane where it is distributed to the dial shelf controller card(s) and feature cards.

The AC-input power shelf includes two 2,000-watt, AC-input power supplies that plug into a common power backplane in the AC-input power shelf. A single AC-input power supply is capable of powering a fully configured Cisco 5814 dial shelf. The second power supply provides full redundancy.

Cisco AS5800/Voice Gateway

The Cisco AS5800/Voice Gateway enables highly scalable deployment of toll-quality voice and fax services over data networks. Enhanced with Cisco's IOS software and Service Node (SN) capabilities, the AS5800 supports features such as pre-paid and post-paid calling card, 800 call redirect, voice activated dialing, and voice and fax mail.

The AS5800 is specifically designed to meet the demands of large service providers such as Post, Telephone, and Telegraphs (PTTs), regional bell operating companies (RBOCs), inter-exchange carriers (IXCs), and large Internet telephony service providers (ITSPs). The physical architecture of the AS5800 product enhances reliability, availability, and serviceability. Critical features to dial POP administrators include minimizing downtime, service costs, and time to deployment.

The AS5800 supports up to 1344 voice ports in a single system, thus offering the highest concentration of VoIP Digital Signal Processors (DSPs) available in a single voice gateway. The AS5800 offers breakthrough voice quality, density, and scalability, while continuing to provide the rich set of access, VoIP, and QoS services that are part of Cisco IOS software.

AS5800 Voice Feature Card

Cisco AS5800 Voice Feature card, is a full featured voice processing card that supports up to 192 DSP-based voice ports. Voice processing capabilities include Voice Activity Detection (VAD), comfort noise generation, adaptive jitter buffering, programmable 16 and 32msec echo cancellation, programmable frame size, and DTMF (Dual Tone Multiple Frequency) detection and generation. The AS5800 Voice Feature card offers industry-leading DSP density and a wide range of VoIP codecs, including G.711, G.729, G.729a, G.723.1, and Group III real-time fax support, on any port at any time.

For more information on the Cisco AS5800, refer to the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide (DOC-5800-SICG)* or the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide (DOC-5800-HICG)* that shipped with your system.

For information on new features and Cisco IOS commands supported by Release 12.0 T, see the "New and Changed Information" section on page 11 and "Related Documentation" section on page 24.

System Requirements

This section describes the system requirements for Release 12.0(7)T:

- Memory Requirements, page 4
- Hardware Supported, page 4
- Modem Code, page 5
- Determining the Software Version, page 5
- Feature Set Tables, page 6

Memory Requirements

Table 1 describes the memory requirements for the Cisco AS5800 feature sets supported by Cisco IOS Release 12.0(7)T. Flash memory is optional for these Cisco AS5800 images.

Table 1 Cisco AS5800 Memory Requirements

System Components	Feature Set	Image Name	Software Image	Minimum Flash	Minimum DRAM
Cisco AS5800	IP Standard	IP Plus	c5800-p4-mz	16 MB	<ul style="list-style-type: none">• 128 MB for NPE-200• 256 MB for NPE-300
Dial Shelf: Cisco 5814		IP Plus	dsc-c5800-mz	8 MB	32 MB
Cisco AS5800	Service Provider Standard	Service Provider IPsec 56	c5800-p456i-mz	16 MB	<ul style="list-style-type: none">• 128 MB for NPE-200• 256 MB for NPE-300

Hardware Supported

The Cisco AS5800 universal access server includes:

Platforms

- Cisco AS5814
- Cisco RS7206
- Cisco RS7206 VXR

Interfaces

- 12 port T 1 or E1 termination card
- 1- port Channelized T 3 (CT3) termination card

Modem Cards

- 72-port modem card
- 144-modem MICA card

Voice Feature Card(VFC)

Supports up to 192 DSP-based voice ports

Optional AC-input Power Shelf

Two AC-input power supplies

NPE Support

With *any* AS5800 software image, the maximum hardware configuration with an NPE-200 router shelf (RS7206) is one CT3 or two T 1/E 1 trunk cards and five DMMs or 10 HMMs for a maximum of 28 T 1/24 E 1 controllers and 720 modems.

If a larger configuration is desired, a second NPE-200 router shelf can be configured in split-shelf mode, or a single NPE-300 (RS7206 VXR).

The NPE call limitations for an AS5800/Voice Gateway are:

- 672 calls per NPE-200
- 1344 calls per NPE-300

Modem Code

Modem code, which is firmware or portware, runs on the MICA 72- and 144-modem (6- and 12-port) modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the access server starts, the Cisco IOS software unpacks the modem code and loads the proper code on the modem cards. Table 2 lists the current bundled modem code versions.

Table 2 Current Modem Versions

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

Note The Cisco factory could have installed a later version of modem code than the one bundled with the Cisco IOS software. When this happens, the factory installs modem code in Flash memory and maps that code 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 CCO and on the Documentation CD-ROM.

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5800: Port Firmware

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800: Firmware/Portware Release Notes

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5800, log in to the Cisco AS5800 and enter the **show version EXEC** command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5800 Software (c5800-p4-mz), Version 12.0(7)T, RELEASE SOFTWARE
```

Updating to a New Release

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

Service & Support: Product Bulletins: Software

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

Feature Set Tables

The Cisco AS5800 universal access server contains multiple Cisco IOS software images. Table 3 lists the software images which require part numbers for ordering.

Table 3 Cisco IOS Software Images

Software Image	Description
c5800-p4-mz	Router shelf image—Cisco IOS software image supporting the Cisco 7206 router shelf functionality, bundled trunk card, and modem card images.
c5800-p456i-mz	Router shelf image—Same as c5800-p4-mz with enhanced security features for service providers.
dsc-c5800-mz	Dial shelf controller image—Special image for the Cisco 5814 dial shelf controller card



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.

Table 4 lists the features and feature sets supported by the Cisco IOS Release 12.0 T for the Cisco AS5200. This table uses the following conventions to identify features:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (7) means a feature was introduced in 12.0(7)T. If a cell in this column is empty, the feature was included in the initial base release.

Note This feature set table contains only a selected list of features. This table is not a cumulative nor complete list of all the features in each image

Table 4 Feature List by Feature Set for the Cisco AS5800 Access Servers

Features	Feature Set		
	In	IP Plus	IPSEC 56
CT3 Channelized T3 Trunk Card	(3)	Yes	No
DSC Redundancy, Phase I	(3)	Yes	No

Table 4 Feature List by Feature Set for the Cisco AS5800 Access Servers (continued)

Features	Feature Set		
	In	IP Plus	IPSEC 56
Policy Routing Infrastructure Update	(3)	Yes	Yes
Process MIB	(3)	Yes	No
Cisco IOS Support for IP Connection to SS7 Signalling Controller	(3)	Yes	No
IBM Support			
APPN High-Performance Routing	—	No	No
APPN MIB Enhancements	—	No	No
APPN over Ethernet LAN Emulation	—	No	No
APPN Scalability Enhancements	—	No	No
Bisync Enhancements	—	No	No
Cisco MultiPath Channel (CMPC)	—	No	No
DLSw+ Enhancements	—	No	No
FRAS Enhancements	—	No	No
RIF Passthru in DLSw+	—	No	No
SRB over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers	—	No	No
TN3270 LU Nailing	—	No	No
TN3270 Server Enhancements	—	No	No
Token Ring LANE	—	No	No
Tunneling of Asynchronous Security Protocols	—	No	No
Internet			No
Async over UDP	(5)	Yes	Yes
DRP Server Agent	—	No	No
DRP Server Agent Enhancements	—	No	No
IP Routing			No
Easy IP (Phase 1)	(1)	Yes	No
DHCP Server for Easy IP	(1)	Yes	Yes
HSRP over ISL in Virtual LAN Configurations	—	No	No
IP Enhanced IGRP Route Authentication	(1)	Yes	No
OSPF LSA Group Pacing	(1)	Yes	No
OSPF Point-to-Multipoint Networks with Neighbors	(1)	Yes	No
Per User DNS	-	Yes	Yes
PIM Version 2	(1)	Yes	No
TCP Enhancements:	(1)	Yes	No
— TCP Selective Acknowledgment			
— TCP Timestamp			
LAN Support			No
AppleTalk Access List Enhancements	—	No	No
DECnet Accounting	—	No	No

Table 4 Feature List by Feature Set for the Cisco AS5800 Access Servers (continued)

Features	Feature Set		
	In	IP Plus	IPSEC 56
IPX Named Access Lists	—	No	No
IPX SAP-after-RIP	—	No	No
NLSP Enhancements	—	No	No
NLSP Multicast Support	—	No	No
Management			No
Cisco Call History MIB Command Line Interface	(1)	Yes	Yes
Cisco IOS File System	(1)	Yes	Yes
Cisco IOS Internationalization	(1)	Yes	Yes
CLI String Search	(1)	Yes	Yes
Conditionally Triggered Debugging	(1)	Yes	Yes
Dial Shelf Controller Redundancy	(3)	Yes	Yes
Entity MIB, Phase 1	(1)	Yes	Yes
External Portware Download	—	Yes	Yes
Parse Bookmarks	(1)	Yes	Yes
Process MIB	(3)	Yes	Yes
Show Caller Command	—	Yes	Yes
Show Modem Command	—	Yes	Yes
SNMP v2C	(1)	Yes	Yes
SNMP v3	(3)	Yes	Yes
SNMP Inform Requests	—	Yes	Yes
Virtual Profiles	(1)	Yes	Yes
VPDN MIB	(1)	Yes	Yes
VPDN MIB and Syslog Facility	—	Yes	Yes
Multimedia			
IP Multicast Load Splitting across Equal-Cost Paths	(1)	Yes	No
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	(1)	Yes	No
IP Multicast over Token Ring LANs	(1)	Yes	No
Stub IP Multicast Routing	(1)	Yes	No
Quality of Service			
RTP Header Compression	—	Yes	Yes
Security			
AAA Scalability	—	Yes	Yes
Authenticating ACL	—	No	No
Automated Double Authentication	—	No	No
Certificate Authority Interoperability	—	No	No
Double Authentication	(1)	Yes	No

Table 4 Feature List by Feature Set for the Cisco AS5800 Access Servers (continued)

Features	Feature Set		
	In	IP Plus	IPSEC 56
Encrypted Kerberized Telnet	—	Yes	Yes
HTTP Security	(1)	Yes	No
Internet Key Exchange Security Protocol	—	No	No
IPSec Network Security	—	No	No
MS-CHAP Support	—	Yes	Yes
Named Method Lists for AAA Authentication and Accounting	—	Yes	Yes
Per-User Configuration	(1)	Yes	No
Reflexive Access Lists	(1)	Yes	No
TCP Intercept	—	No	No
Vendor-Proprietary RADIUS Attributes	(1)	Yes	Yes
Vendor-Proprietary RADIUS -Additional Attributes	-	No	No
Switching			
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	—	No	No
CLNS and DECnet Fast Switching over PPP	—	No	No
DECnet/Vines/XNS over ISL	—	No	No
Fast-Switched Policy Routing	(1)	Yes	No
IPX Routing over ISL Virtual LANs	—	No	No
VIP Distributed Switching Support for IP Encapsulated in ISL	—	No	No
Terminal Services			
Telnet Extensions for Dialout	—	Yes	Yes
Virtual Templates for Protocol Translation	—	Yes	Yes
WAN Optimization			
ATM MIB Enhancements	—	No	No
PAD Enhancements	—	No	No
PAD Subaddressing	(1)	Yes	No
WAN Services			
Always On/Dynamic ISDN (AO/DI)	—	Yes	Yes
Bandwidth Allocation Control Protocol	(1)	Yes	No
Channelized T3	—	Yes	Yes
Dialer Watch	(1)	Yes	No
E1 R2	(3)	Yes	No
E1 R1 Support for Taiwan only	(3)	Yes	No
Enhanced Local Management Interface (ELMI)	—	No	No
Frame Relay Enhancements	(1)	Yes	No
Frame Relay MIB Extensions	(1)	Yes	No
Frame Relay Router ForeSight	(1)	Yes	No

Table 4 Feature List by Feature Set for the Cisco AS5800 Access Servers (continued)

Features	Feature Set		
	In	IP Plus	IPSEC 56
GRE VPN	—	Yes	Yes
ISDN Advice of Charge	(1)	Yes	No
ISDN Caller ID Callback	(1)	Yes	No
ISDN NFAS	(1)	Yes	No
Layer 2 Forwarding—Fast Switching	(1)	Yes	No
Layer 2 Tunneling Protocol	(1)	Yes	Yes
L2TP Dial Out	(5)	Yes	Yes
Leased-Line ISDN at 128 kbps	—	No	No
Microsoft Point-to-Point Compression (MPPC)	—	Yes	Yes
MS Callback	(1)	Yes	No
Modem Management Enhancements	(1)	Yes	No
Multiple ISDN Switch Types	—	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces (NI2)	—	Yes	Yes
PPP over ATM	—	No	No
SS7	(4)	Yes	Yes
Stackable Home Gateway	—	No	No
Switched 56K Digital Connections	—	Yes	Yes
Telnet Extensions for Dialout	—	Yes	Yes
X.25 Enhancements	(1)	Yes	No
X.25 on ISDN	(1)	Yes	No
Miscellaneous			
Policy Routing Infrastructure	(3)	Yes	Yes
Resource Pool Management	(5)	Yes	Yes
Subnetwork Bandwidth Manager	(5)	Yes	Yes
New			
AS5800/Voice Gateway	(7)	Yes	Yes
Configuring RADIUS for Multiple User Datagram Protocol Ports	(7)	Yes	Yes
Dynamic Multiple Encaps for Dial-In over ISDN	(7)	Yes	Yes
Resource Pool Management Server	(7)	Yes	Yes
Resource Pool Management with Direct Remote Services	(7)	Yes	Yes
Selecting AAA Server Groups Based on DNIS	(7)	Yes	Yes

New and Changed Information

This section lists the new features supported by the Cisco AS5800 for Cisco IOS in Release 12.0 T.

New Hardware Features in Release 12.0(7)T

The following new hardware features are supported by the Cisco AS5800 for Release 12.0(7)T:

AS5800/Voice Gateway

The AS5800/Voice Gateway converts and routes voice and fax calls between traditional circuit-switched networks and packet-switched networks. When equipped with AS5800 Voice Feature Cards (TI C549 DSP-based Voice Feature Card) and an H.323 voice-enabled Cisco IOS feature license, the AS5800 serves as a high-performance, carrier-class, H.323-compliant voice gateway. In other words, it provides the conversion and routing of voice and fax calls between central office (CO) switches/PBXs and IP networks for service provider and enterprise applications. Although Cisco offers a variety of voice gateway solutions for carrying voice over IP, ATM and Frame Relay networks, the AS5x00s are specifically designed and optimized for IP applications.

New Software Features in Cisco IOS Release 12.0(7)T

The following new hardware features are supported by the Cisco AS5800 universal access servers for Release 12.0(7)T:

Cisco H.235 Accounting and Security Enhancements for Cisco Gateways

The Cisco H.323 gateway now supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 and is used in a “password-with-hashing” security scheme described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message and is used to authenticate the sender of the message. You can use a separate database for user ID and password verification.

With this release, Cisco H.323 gateways support three levels of authentication:

- **Endpoint**—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communications, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.
- **Per-Call**—When the gateway receives a call over the telephony leg, it prompts the user for an account number and personal identification number (PIN). These two numbers are included in certain RAS messages sent from the endpoint and are used to authenticate the originator of the call.
- **All**—This option is a combination of the other two. With this option, the validation of cryptoTokens in ARQ messages is based on an the account number and PIN of the user making a call and the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

You can configure the level of authentication for the gateway using the Cisco IOS software command line interface.

CryptoTokens for registration requests (RRQ), unregistration request (URQ), disengage request (DRQ) and the terminating side of admission request (ARQ) messages contain information about the gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the gateway) and the gateway password. CryptoTokens for the originating side ARQ messages contain information about the user that is placing the call, including the user ID and personal identification number (PIN).

Cisco H.323 Multizone Enhancements

Cisco H.323 Multizone enhancements allow a Cisco gateway to provide information to the gatekeeper with additional fields in the RAS (registration, admission, and status) messages.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an Admission Confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

This version of the H.323 software adds support to allow a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF. The gateway will include the canMapAlias associated destination information in setting up the call to the destination gateway.

In conjunction with the canMapAlias functionality, this version includes support for the gatekeeper to indicate to the gateway that the call should be destined to a new E.164 number. The gatekeeper indicates this by sending an Admission Confirm message with an IP address of 0.0.0.0 in the destCallSignalAddress field and the new destination E.164 phone number in the destinationInfo field.

The gateway receiving such an ACF will fall back to routing the call based on this new E.164 address and performing a new lookup of the gateway's configured dial plan. This may result in the call being routed back to the PSTN or to an H.323 endpoint.

Configuring RADIUS for Multiple User Datagram Protocol Ports

In past Cisco IOS releases, RADIUS hosts were uniquely identified by their IP addresses; therefore, only one definition of a RADIUS server for each IP address was allowed. The Configuring RADIUS for Multiple UDP Ports feature expands RADIUS implementation so that RADIUS security servers are identified by their IP addresses and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

The Configuring RADIUS for Multiple UDP Ports feature also applies to RADIUS server groups—server groups can now include multiple service definitions for host entries for the same server, as long as each entry has a unique identifier.

Dynamic Multiple Encapsulations for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on calling line identification (CLID) or DNIS. It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID (caller ID) or DNIS to ensure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

In addition, a large set of user profiles can be stored in dialer profiles locally or on a remote AAA server. (For large scale dial-in, storing user-specific configurations on a remote server becomes necessary for enhancing expandability and local memory efficiency.) However, whether stored locally or on a remote AAA server, the user-specific encapsulation and configuration can be applied to individual B channels dynamically and independently.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Gateway Support for Alternate Gatekeeper

The Alternate Gatekeeper feature provides redundancy for a gatekeeper in a system where gatekeepers are used. This enhancement allows a gateway to use up to two alternate gatekeepers as a backup in the case of a primary gatekeeper failure.

A gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gateway and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path, to provide connectivity with the public switched telephone network (PSTN), to improve Quality of Service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS) or using Cisco IOS configuration options.

Redundant Link Manager

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Redundant Link Manager (RLM) provides link management over multiple IP networks, so that your Cisco SS7 DAS can tolerate a single point of failure.

By using the RLM functionality, the Q.931 signaling protocol and other proprietary protocols are transported on top of multiple redundant links between a telephony controller and the media gateways (MGWs).

A feature enhancement to RLM for this Cisco SS7 DAS release is redundancy at the link and telephony-controller level. When each RLM group has multiple telephony controllers associated with a MGW, a telephony-controller priority and a link priority are examined by the RLM client during failover, ensuring improved control handling. The RLM client is an MGW running RLM software.

The RLM client on the MGW supports both versions of RLM functionality:

- Multiple redundant links between a single telephony-controller and the MGWs (Version 1)
- Multiple redundant links between multiple telephony-controllers and the MGWs (Version 2)

After installation, the RLM client defaults to Version 2; however, you can choose a different version by using a command line interface (CLI) configuration command. Once an RLM version is selected, all RLM groups on a given MGW use the selected version's functionality.

Note The RLM feature is backwards compatible on the telephony-controller, but only one version of the RLM client can run on a given MGW.

Resource Pool Management Server

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Resource Pool Manager Server (RPMS) communicates with the RPM component of the MGWs to enable telephone companies and ISPs to count, control, bill, and manage resources centrally for wholesale and retail dial network services. RPM is configured across multiple MGW stacks using one or more external RPMS.

The Cisco RPMS provides the following:

- Customer shared-resource management
- Advanced wholesale (VPDN) services for enterprise accounts and ISPs
- Efficient use of resources to offer different oversubscription ratios and dial-service agreements
- Combination of retail and wholesale services on the same MGWs

Cisco RPMS offers three major functions:

- Resource management uses the call type and dialed number identification service (DNIS) information to accept or reject the call based on the customer profile session limits associated with the DNIS information. If the call is accepted, the call is assigned to an MGW resource.
- Dial services determines how the call is handled after it is answered. The call can be authenticated locally or sent to a home gateway through a VPDN tunnel (using the DNIS information or a domain name).
- Call discrimination is used to prevent unapproved call types from accessing MGW resources. When a call is placed, the MGW sends the call type and dialed number information service (DNIS) information to the Cisco RPMS. The Cisco RPMS compares this combination to the call discrimination table. If the call type-DNIS combination appears in the table, the call is rejected.

Resource Pool Management with Direct Remote Services

Cisco Resource Pool Manager (RPM) enables telephone companies and ISPs to share dial resources for wholesale and retail dial network services in a single network access server (NAS) or across multiple NAS stacks. With Cisco RPM, service providers can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements.

Cisco RPM can be configured in one or more standalone Cisco NASs, or, optionally, across multiple NAS stacks by using one or more external Cisco Resource Pool Manager Servers (RPMSs).

The Cisco RPM is ideal for combining retail and wholesale dial services using Cisco AS5200, AS5300, and AS5800 network access servers. Call management and call discrimination can be configured to occur before the call is answered. Dial customers are differentiated by the use of configurable customer profiles that are based on the Dialed Number Information Service (DNIS) and the call type determined at the time of an incoming call. When a call arrives at the NAS, the DNIS and call type are matched against a table of disallowed calls. If the DNIS and call type match an entry in this table, the call is rejected. Call discrimination can be used to manage the billing of calls to different types of resources.

When management by virtual private dialup network (VPDN) is configured, a VPDN group includes the information needed to set up or reject a VPDN session. VPDN setup can be based on the DNIS received during call setup, or on the domain name after the call is answered. Load balancing is used to achieve full usage of VPDN tunnels. The VPDN group can also serve as the “customer profile” when all calls are answered and sessions are identified and limited by domain name instead of DNIS.

To support data over voice bearer service (DoVBS), service providers use DNIS to direct calls to the appropriate resource. When a digital call arrives at the NAS through the voice network, it terminates on a High-Level Data Link Control (HDLC) controller rather than on a modem.

Direct remote services is an enhancement to Cisco resource pool management (RPM) implemented in Cisco IOS Release 12.0(7)T that enables service providers to implement wholesale dial services without using VPDN tunnels. A customer profile that has been preconfigured with a PPP template to define the unique PPP services for the wholesale dial customer is selected by the incoming DNIS and call type. At the same time, the DNIS is used to select AAA server groups for authentication/authorization and for accounting for the customer.

Selecting AAA Server Groups Based on DNIS

In past Cisco IOS releases, authentication and accounting services (otherwise referred to as AAA services) have been implemented in one of the following methods:

- Globally—meaning that AAA services were defined using global configuration access list commands and applied in general to all interfaces on a specific network access server
- Per Interface—meaning that AAA services were defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server
- Using the AAA DNIS Map feature as described in the Cisco IOS Release 12.0(2)T *Selecting AAA Servers Using DNIS Numbers* feature module—meaning that you could use DNIS to specify one AAA server to supply AAA services

With Cisco IOS Release 12.0(7)T, you can now select an AAA server group to which authentication and accounting requests will be sent by using DNIS. With this new Selecting AAA Server Groups Based on DNIS feature, you can specify the same server group for AAA services or a separate server group for each AAA service. You can now configure authentication and accounting on different physical devices and provide failover backup support.

This feature obsoletes the previous Cisco IOS Release 12.0(2)T AAA DNIS Map feature.

New Software Features in Cisco IOS Release 12.0(5)T

The following new hardware features are supported by the Cisco AS5800 universal access servers for Release 12.0(5)T:

Asynchronous Serial Traffic over UDP

The Asynchronous Serial Traffic over UDP feature provides the ability to encapsulate asynchronous data into UDP packets, and then unreliably send this data without needing to establish a connection with a receiving device.

You load the data you want to send through an asynchronous port, and then send it, optionally, as a multicast or a broadcast. The receiving device(s) can then receive the data whenever it wants. If the receiver ends reception, the transmission is unaffected.

This process is referred to as UDP Telnet (UDPTN), although it does not (and cannot) use the Telnet protocol. UDPTN is similar to Telnet in that both are used to send data, but UDPTN is unique in that it does not require that a connection be established with a receiving device.

Cisco Resource Pool Manager

The Cisco Resource Pool Manager (RPM) feature enables telephone companies and Internet service providers (ISPs) to share dial resources for wholesale and retail dial network services. With RPM, telcos and ISPs can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements. Resource pool management can be configured in a single, standalone Cisco network access server using RPM or, optionally, across multiple network access server stacks using one or more external Cisco Resource Pool Manager Servers.

Service Assurance Agent

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 by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to:

- Monitor the Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signalling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signalling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signalling method is similar to that of RSVP itself. SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

No Cisco IOS Release 12.0(4)T for the AS5800

There was no Cisco IOS Release 12.0(4)T for the AS5800.

New Software Features in Cisco IOS Release 12.0(3)T

The following software enhancement is available for the Cisco MC3810 in Cisco IOS Release 12.0(3)T.

Cisco IOS SNMPv3

Cisco IOS Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID, which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- **Modification of Information** or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal
- **Masquerade** or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- **Message Stream Modification** or protection against messages getting maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations
- **Disclosure** or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy. They are:
 - communication without authentication and privacy (NoAuthNoPriv)
 - communication with authentication and without privacy (AuthNoPriv)
 - communication with authentication and privacy (AuthPriv)

Cisco IOS Support for IP Connection to SS7 Signalling Controller

This release allows carrier customers to connect their access servers to the Public Switch Telephone Network (PSTN) directly by using Signaling System #7 (SS7) signaling protocols. The SS7 signaling links terminate on a separate Unix system called the Signaling Controller (SC2200). The SC2200 maps incoming calls, which are signaled via SS7, to bearers on the access servers. The access servers and SC2200 interact to set up and tear down calls using and extended Q.931 protocol over Q.921 and UDP. In this manner, the access servers and SC2200 form a system that emulates an end-office switch in the PSTN.

The Cisco IOS Support for IP Connection to SS7 Signalling Controller adds two capabilities to IOS. The control protocol implementation (Q.931/Q.921 over UDP) and Continuity Check (the ability to loop back a DS-0 and generate tones) which is a maintenance function used in some networks.

In addition to remote access, SS7 is critical for Carrier-Class voice applications. With SS7 and voice functionality combined, Cisco's products are on a roadmap toward the direct integration of Cisco voice products within the public telephony network, a core strategic direction for Cisco.

Cisco Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by SNMP. The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

DSC Redundancy

The dial shelf may contain two DSC cards. A DSC card provides a master clock for the dial shelf, the fast ethernet link to the router shelf, environmental monitoring of the feature boards, and the feature boards with bootstrap images on start-up. With two DSC cards present, we have the possibility of DSC redundancy where one DSC will act as a backup to the active one. When the active DSC fails the backup will provide the functionality as well as increase system availability by preventing loss of service in the event of the failure of one of the DSCs.

Policy Routing Infrastructure Update

This update provides full support of IP Policy Based Routing in conjunction with Cisco Express Forwarding and NetFlow. As CEF gradually obsoletes fast switching, policy routing must be integrated with CEF to meet customer performance requirements. When both policy routing and flow are enabled, redundant processing will be avoided to optimize performance and deliver a scalable set of services.

T3/DS3 Ingress Interface to CT3

The primary purpose of this card is to provide aggregation of channelized interfaces into the CT3 on a single T3 facility. This will allow for increased port density, lower per port cost, ease of deployment, ease of provisioning, etc. which all lead to an overall lower cost of ownership to the customer.

T3 refers to a 672 channel interface as defined in the North American T-Carrier Hierarchy. T-Carrier represents one of several multiplexed carrier systems, three of which are listed below. Each T-Carrier level is also commonly referred to by an appropriate Digital Signal (DS) level which is also listed. The following provides the overall data rate and channel capacity of each level in the North American T-Carrier Hierarchy

- T/DS Level Data Rate (bps) voice channels
- T1 (DS 1) 1.544 Mbps 24
- T2 (DS 2) 6.312 Mbps 96
- T3 (DS 3) 44.736 Mbps 672

The T2 standard is very seldom (if ever) used today while services based on T1 and T3 are widely available. The current CT3 product offers individual T1 interfaces for a total of 24 each. By including a T3 interface to the product, offering we gain port density in that 28 T1s will be supported in the same chassis.

Due to the physical constraints of the CT3 chassis, a CT3 interface card is the only way to fully utilize extra modem capacity. To double the CT3 capacity two to each T3s or 1344 modems, two CT3 cards per CT3 chassis would be required.

New Software Features in Release 12.0(2)T

The following new features for the Cisco AS5800 universal access server are available for Cisco IOS Release 12.0(2)T. Documentation is provided separately for these features.

- E1 R1 Signaling for Cisco AS5800 Access Servers
- E1 R2 Signaling for Cisco AS5800 Access Servers

E1 R1 Signaling for Cisco AS5800 Access Servers

Enabling R1 Modified Signaling allows a Cisco AS5800 universal access server to talk to central office trunks that also use R1 Modified Signaling. R1 Signaling is an international signaling standard that is common to channelized T1/E1 networks; however, Cisco only has made this feature available in Taiwan. You can configure a channelized T1/E1 interface to support different types of R1 Modified Signaling, which is used in older analog telephone networks.

Note This type of signaling is not the same as ITU R1 signaling; it is R1 signaling modified for Taiwan specifically.

Note In the future, R1 Modified Signaling will be available in Turkey as well as Taiwan.

E1 R2 Signaling for Cisco AS5800 Access Servers

R2 signaling is an international signaling standard that is common to channelized E1 networks. However, there is no single signaling standard for R2. The ITU-T Q.400-Q.490 recommendation defines R2, but a number of countries and geographic regions implement R2 in entirely different ways. Cisco Systems addresses this challenge by supporting many localized implementations of R2 signaling in its Cisco IOS software.

Cisco System's E1 R2 signaling default is ITU, which supports the following countries: Denmark, Finland, Germany, Russia (ITU variant), Hong Kong (ITU variant), and South Africa (ITU variant). The expression "ITU variant" means there are multiple R2 signaling types in the specified country, but Cisco supports the ITU variant.

Cisco Systems also supports specific local variants of E1 R2 signaling in the following regions, countries, and corporations:

- Argentina
- Australia
- Brazil
- China
- Columbia
- Costa Rica
- East Europe (includes Croatia, Russia, and Slovak Republic)
- Ecuador ITU
- Ecuador LME
- Greece
- Guatemala
- Hong Kong (uses the China variant)
- Indonesia
- Israel
- Korea
- Malaysia
- New Zealand
- Paraguay
- Peru
- Philippines
- Saudi Arabia
- Singapore
- South Africa (Panaftel variant)
- Telmex corporation (Mexico)
- Telnor corporation (Mexico)
- Thailand
- Uruguay
- Venezuela
- Vietnam

Note Only MICA modems support R2 functionality.

New Software Features in Release 12.0(1)T

The following new features for the Cisco AS5800 universal access server are available for Cisco IOS Release 12.0(1)T.

Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) is an access server authentication, authorization, and accounting (AAA) protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server (NAS) and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes. Users who have implemented security solutions using a vendor-proprietary implementation of RADIUS can now integrate Cisco access servers into their networks more easily.

Microsoft Point-to-Point Compression

Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize processor and bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer, called a dictionary.

MS-CHAP Support

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a NAS.

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set of “reason-for failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without authentication, authorization and accounting (AAA) security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS.

Multiple ISDN Switch Types

The **Multiple ISDN Switch Types** feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global **isdn switch-type** command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

The **isdn tei** command is also extended to the interface level. Terminal endpoint negotiation (TEI) determines when Layer 2 is activated (powerup or first-call).

Named Method Lists for AAA Authorization and Accounting

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco's Authentication, Authorization, and Accounting (AAA) network security services. With Cisco IOS Release 11.3(3)T, AAA has been extended to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication; they allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRIs) and Basic Rate Interfaces (BRIs) as follows:

- Adds a new switch type for PRIs (**isdn switch-type primary-ni**).
- Changes the BRI basic-ni1 switch type to basic-ni (**isdn switch-type basic-ni**).
- Removes the ISDN vn2 switch type (**isdn switch-type vn2**) used in France. The existing vn3 switch type (**isdn switch-type vn3**) supports French vn2 switches.
- Removes the ISDN basic-nwnet3 switch type (**isdn switch-type basic-nwnet3**) used in Norway. The basic-net3 switch type (**isdn switch-type basic-net3**) supports Norway NET3 switches.
- Removes the ISDN basic-nznet3 switch type (**isdn switch-type basic-nznet3**) used by New Zealand NET3 switches. The ISDN basic-net3 switch type (**isdn switch-type basic-net3**) supports New Zealand NET3 switches.
- Adds the ability to configure outgoing PRI B-channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Note The command parser will still accept the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration using either the **show running configuration** or **write terminal** command, the basic-net3 or vn3 switch types are displayed respectively.

Performance Data Collection

The Performance Data Collection feature allows a Cisco 3640 system controller to collect and store SNMP MIB data from its managed router and dial shelves. The system controller then serves as a central point for network management data collection. The system controller collects the raw data from the managed shelves periodically, saves the data, and provides a single access point for a central network management application. The data can then be uploaded to a network management station using FTP or TFTP.

VPDN MIB and Syslog Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) feature is intended to support all the tables and objects defined in “Cisco VPDN Management MIB” for the user sessions of the VPDN features. There are a number of commands that provide information and statistics through the Command Line Interface (CLI) but not Simple Network Management Protocol (SNMP); the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

Limitations and Restrictions

MIBs

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

Table 5 **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
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	
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	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Important Notes

This section contains important information about Cisco IOS Release 12.0 T software that can apply to the Cisco AS5800 universal access server.

Last Maintenance Release of Cisco IOS Release 12.0 T

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

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

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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

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

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

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

Related Documentation

The following sections describe the documentation available for the Cisco AS5800 universal access servers. 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 25
- Platform-Specific Documents, page 26
- Feature Modules, page 27
- Cisco IOS Software Documentation Set, page 27

Release-Specific Documents

The following documents are specific to Release 12.0(7)T. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.0 T*

You can reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO at:

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

You can reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM at:

Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.0 T

- Product bulletins, field notices, and other release-specific documents

You can reach these documents on CCO at:

Technical Documents: Product Bulletins

- Caveat documents

As a supplement to the caveats listed in the “Caveats” section in these release notes, see the *Caveats for Cisco IOS Release 12.0 T* document, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

You can reach the caveat document on CCO at:

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

You can reach the caveat document on the Documentation CD-ROM at:

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

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

Platform-Specific Documents

These documents are available for the Cisco AS5800 universal access servers on CCO and the Documentation CD-ROM: .

Table 6 Cisco AS5800 Universal Access Server—Related Documents

Cisco Product	Document Title
Cisco AS5800 universal access server	<ul style="list-style-type: none"> • <i>Cisco AS5800 Universal Access Server Hardware Installation and Configuration Guide</i> • <i>Cisco AS5800 Universal Access Server Regulatory Compliance and Safety Information</i> • Configuration notes, updates, feature modules, and release notes
Cisco 7206 router shelf	<ul style="list-style-type: none"> • <i>Cisco 7206 Installation and Configuration Guide</i> • <i>Regulatory Compliance and Safety Information for the Cisco 7206</i> • Configuration notes, updates, feature modules, and release notes
Cisco 3640 system controller	<ul style="list-style-type: none"> • <i>Cisco 3640 Router Installation and Configuration Guide</i> • <i>Cisco 3640 System Controller Installation and Configuration Guide</i> • <i>Regulatory Compliance and Safety Information for the Cisco 3640</i> • Configuration notes, updates, feature modules, and release notes
Cisco IOS software	<ul style="list-style-type: none"> • Configuration guides • Command references • Feature modules, configuration notes, updates, and release notes
Cisco marketing tools	<ul style="list-style-type: none"> • <i>Cisco Information Packet</i> • <i>Cisco Product Catalog</i> • <i>Cisco Product Bulletin 738</i>

This documentation can be found on CCO and the Documentation CD-ROM:

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5800

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800

Feature Modules

Feature modules describe new features supported by Release 12.0 T and are an update to the Cisco IOS documentation set. They consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. The feature module information is included in the next printing of the Cisco IOS documentation set.

On CCO at:

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

On the Documentation CD-ROM at:

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

You can reach these documents on CCO at:

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

You can reach these documents on the Documentation CD-ROM at:

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

Release 12.0 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

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

Related Documentation

You can reach the Cisco IOS documentation set on CCO at:

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

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

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

Table 7 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Configuration Guide</i> 	Interface Configurations
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 7 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> 	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
<ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> 	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none"> • <i>Configuration Guide Master Index</i> • <i>Command Reference Master Index</i> 	
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Cisco IOS System Error Messages</i> • <i>Debug Command Reference</i> • <i>Dial Solutions Quick Configuration Guide</i> 	

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

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

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

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: 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 and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@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, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used with the documents described in the section ““Related Documentation,” page 24.”

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, Wavelength Router, Wavelength Router Protocol, WaRP, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (9911R)

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