



Release Notes for Cisco AS5350 Universal Gateways for Cisco IOS Release 12.1 XM

February 25, 2002

Cisco IOS Release 12.1(5) XM8

78-12053-01 Rev. J0

These release notes for the Cisco AS5350 universal gateways describe the enhancements provided in Cisco IOS Release 12.1(5) XM8. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1(5) XM8, see the [“Caveats for Cisco IOS Release 12.1 XM” section on page 23](#) and *Caveats for Cisco IOS Release 12.1T*. This caveats document is updated for every maintenance release and is also located 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 7](#)
- [Limitations and Restrictions, page 23](#)
- [Caveats for Cisco IOS Release 12.1 XM, page 23](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation, page 33](#)
- [Cisco IOS Software Documentation Set, page 30](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco AS5350 Universal Gateway is the only one-rack-unit, two, four, or eight PRI gateway that provides universal services— data, voice, and fax services on any service, any port. The Cisco AS5350 offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprises that require innovative universal services.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.1(5) XM8, see the [“New and Changed Information” section on page 7](#) and the [“Related Documentation” section on page 28](#).

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(5) XM8:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 4](#)

Memory Recommendations

Table 1 *Memory Recommendations for the Cisco AS5350 Universal Gateways*

Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
IP Plus	c5350-is-mz	32 MB	128 MB	RAM
IPSec 56	c5350-is56i-mz	32 MB ¹	128 MB	RAM
Enterprise Plus	c5350-js-mz	32 MB	128 MB	RAM
Enterprise IPSec 56	c5350-js56i-mz	32 MB ¹	128 MB	RAM

1. Flash is optional.

Supported Hardware

Cisco IOS Release 12.1(5) XM8 supports the Cisco AS5350. [Table 2](#) lists the interfaces and supported dial feature cards.

For detailed descriptions of the new hardware features, see the “[New and Changed Information](#)” section on [page 7](#).

Table 2 Supported Interfaces for the Cisco AS5350

Interfaces and Dial Feature Cards	Product Description
Dial Feature Cards	AS535-DFC-60NP
	AS54-DFC-108NP
LAN Interfaces	Fast Ethernet 10/100BaseT (RJ-45)
Trunk/Backhaul Interface Options	2PRI CT1/CE1 DFC Two 8MB Serial ports
	4PRI CT1/CE1 DFC
	8PRI CT1/CE1 DFC

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5350, log in to the Cisco AS5350 and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software (c5350-is-mz), Version 12.1(5) XM8, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Other Firmware Code

Default bundled firmware for Nextport upgraded from version 2.3.3.108 to version 2.3.5.108.

Feature Set Tables

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

Cisco IOS Release 12.1(5) XM8 supports the same feature sets as Cisco IOS Release 12.1(5) T, but Cisco IOS Release 12.1(5) XM8 can include new features supported by the Cisco AS5350.



Note

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>.



Caution

Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple DataEncryption Standard [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 because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 lists the features and feature sets supported by the Cisco AS5350 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.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (5) T means a feature was introduced in 12.1(5) T.



Note

This table might not be cumulative or list all the features in each image. 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 3 Feature List by Feature Set for the Cisco AS5350

Feature	In	Software Images by Feature Set			
		IP Plus	IP Plus IPsec 56	Enterprise Plus	Enterprise Plus IPsec 56
Dial					
Call Admission Control Based on CPU Utilization	(5)XM2	Yes	No	Yes	Yes
Cisco Resource Pool Manager CLID/DNIS Call Discriminator	(5)T	Yes	No	Yes	No
Dial Peer Enhancements	(5)XM2	Yes	No	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5350

Feature	In	Software Images by Feature Set			
		IP Plus	IP Plus IPsec 56	Enterprise Plus	Enterprise Plus IPsec 56
ISDN Network Side for ETSI Net5 PRI	(5)XM2	Yes	Yes	Yes	Yes
Monitoring Resource Availability on Cisco AS5300, AS5400, and AS5800 Universal Access Servers	(5)T	Yes	No	Yes	No
NTT PRI NFAS	(5)XM2	Yes	Yes	Yes	Yes
Setting the Port Threshold for the Trunk Card	(5)T	Yes	Yes	Yes	Yes
File or System Management					
AutoInstall Using DHCP for LAN Interfaces (CSCdr88175)	(5)T	Yes	No	Yes	No
Cisco Resource Pool Manager CLID/DNIS Call Discriminator	(5)T	Yes	Yes	Yes	Yes
Ethernet-like Interfaces MIB and Interfaces Group MIB Enhancements	(5)T	Yes	Yes	Yes	Yes
Event MIB	(5)T	Yes	Yes	Yes	Yes
Individual SNMP Trap Support	(5)T	Yes	Yes	Yes	Yes
Individual SNMP Trap Support	(5)T	Yes	Yes	Yes	Yes
MSDP MIB	(5)T	Yes	Yes	Yes	Yes
NextPort Port Service Management for the Cisco AS5400 Universal Access Server	(5)T	Yes	No	Yes	No
WCCP Redirection on Inbound Interfaces	(5)T	Yes	No	Yes	No
Interfaces					
Individual SNMP Trap Support	(5)T	Yes	Yes	Yes	Yes
Interface Range Specification	(5)T	Yes	Yes	Yes	Yes
IP					
Cisco Resource Pool Manager CLID/DNIS Call Discriminator	(5)T	Yes	Yes	Yes	Yes
IGMP Version 3	(5)T	Yes	Yes	No	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)T	No	No	Yes	Yes
NAT—Support of H.323 v2 Call Signaling (FastConnect)	(5)T	No	No	Yes	Yes
NAT—Support of IP Phone to Cisco CallManager	(5)T	No	No	Yes	Yes
PIM Dense Mode State Refresh	(5)T	Yes	Yes	Yes	Yes
Redundant Link Manager (RLM)	(5)XM2	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5350

Feature	In	Software Images by Feature Set			
		IP Plus	IP Plus IPsec 56	Enterprise Plus	Enterprise Plus IPsec 56
Security					
AAA Broadcast Accounting	(5)T	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(5)T	Yes	Yes	Yes	Yes
Cisco H.235 Accounting and Security Enhancements for Cisco Gateways	(5)XM2	Yes	No	Yes	Yes
Cisco H.323 Multizone Enhancements	(5)XM2	Yes	No	Yes	Yes
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests	(5)T	Yes	No	Yes	No
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests	(5)T	Yes	Yes	Yes	Yes
Video					
H.323 Support for Virtual Interfaces	(5)XM2	Yes	No	Yes	Yes
Voice					
Configurable Timers in H.225	(5)XM2	Yes	Yes	No	Yes
Cisco H.323 Version 2 Phase 2	(5)XM2	Yes	Yes	No	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(5)XM2	Yes	Yes	No	Yes
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(5)XM2	Yes	Yes	No	Yes
Feature Group D Support	(5)XM2	Yes	Yes	No	Yes
Gateway Support for Alternate Gatekeeper	(5)XM2	Yes	Yes	No	Yes
Gateway-to-Gatekeeper Billing Redundancy	(5)XM2	Yes	Yes	No	Yes
H.323 Enhancements	(5)XM2	Yes	Yes	No	Yes
H.323 Version 2 Support	(5)XM2	Yes	Yes	No	No
Interactive Voice Response for Cisco Access Platforms	(5)XM2	Yes	Yes	No	Yes
Interactive Voice Response Version 2.0 on Cisco VoIP Gateways	(5)XM2	Yes	Yes	No	Yes
Interworking Signaling Enhancements for H.323 VoIP	(5)XM2	Yes	Yes	No	Yes
Monitoring Voice and Fax Services on the Cisco AS5350 and Cisco AS5400 Universal Gateways	(5)XM2	Yes	Yes	No	Yes
Service Provider Features for Voice over IP	(5)MX2	Yes	Yes	No	Yes
Settlement for Packet Voice, Phase 2	(5)XM2	Yes	Yes	No	Yes
SIP Diversion Header Implementation for Redirecting Number (CSCdr72341)	(5)XM2	Yes	Yes	No	Yes

Table 3 Feature List by Feature Set for the Cisco AS5350

Feature	In	Software Images by Feature Set			
		IP Plus	IP Plus IPSec 56	Enterprise Plus	Enterprise Plus IPSec 56
T.38 Fax for Cisco Universal Gateways	(5)XM2	Yes	Yes	No	Yes
Voice over IP Q.SIG Network Transparency	(5)XM2	Yes	Yes	No	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5350 for Cisco IOS Release 12.1(5) XM8.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM8

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM8.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM7

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM7.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM6

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM6.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM5

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM5.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM4

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM4.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM3

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM3.

New Hardware Features in Cisco IOS Release 12.1(5) XM2

The following new hardware is supported by the Cisco AS5350 for Cisco IOS Release 12.1(5) XM2.

NP108 DFC, 8PRI CT1/CE1 DFC, 4PRI CT1/CE1 DFC

Three new feature cards are supported. The NP108 DFC (PN AS535-DFC-108NP) provides 108 universal ports for data and voice. 8PRI CT1/CE1 DFC (PN AS535-DFC-8CT1/CE1) provides 8 T1 or E1 ports. The 4PRI CT1/CE1 DFC (PN AS535-DFC-4CT1/CE1) provides 4 T1 or E1 ports. Card installation instructions can be found at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/53crd/index.htm.

DC Power Supply

The AS5350 universal gateway now supports DC power. Power supply installation instructions can be found at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/hw_inst/spares/4519ps.htm.

New Software Features in Cisco IOS Release 12.1(5) XM2

The following new software features are supported by the Cisco AS5350 for Cisco IOS Release 12.1(5)XM2.

Call Admission Control Based on CPU Utilization

The Call Admission Control for CPU Utilization feature permits Cisco access servers, and Cisco universal gateways to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system CPU load level value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. The feature rejects new digital calls (PRI, CAS, and ISDN), with minor disruption to system users. When the preconfigured call denial threshold is reached, subsequent calls cannot get through and the caller hears a busy tone.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/dt61294.htm.

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 as described in section 10.3.3 of the H.235 specification.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/pul0242x.htm.

Cisco H.323 Multizone Enhancements

This feature enables the Cisco gateway to provide information to the gatekeeper with the use of additional fields in the RAS (registration, admission, and status) messages.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/pul0244x.htm.

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.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pullv2p2.htm.

Configurable Timers in H.225

The H.323 Support for Virtual Interfaces feature allows users to configure the H.225 TCP connection timeout value for all out-going call attempts (on a per VoIP dial-peer basis).

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulcftgm.htm.

Dial Peer Enhancements

The following are the new dial-peer enhancements supported:

- Additional Dial String Symbols

Beginning in this release, additional dial string symbols are supported that you use with the destination-pattern dial-peer configuration command to establish the digit pattern.

- Number-Type Matching

To match on a number type for a dial peer call leg, the numbering-type command is used in dial-peer configuration mode. Number-type matching is supported on Plain Old Telephone Service (POTS), VoIP, VoFR, and VoATM dial peers.

- Digit-Strip Option

When a called number is received and matched to a POTS dial peer, the matched digits are stripped and the remaining digits are forwarded to the voice interface. A new command called digit-strip makes this default behavior an option. The digit-strip option is supported on POTS dial peers only.

- Translation Rule Implementation

When configuring your dial peers, you are provided with an option called the translation rule. This rule applies a translation rule to a calling party number (Automatic Number Identification [ANI]) or a called party number (Dial Number Information Service [DNIS]) for both incoming and outgoing calls within Cisco H.323 voice-enabled gateways. Also, the rule allows translation of the type of number.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldt662.htm.

Ecosystem Gatekeeper Interoperability Enhancements

The H.323 Support for Virtual Interfaces feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection (GRJ) and registration rejection (RRJ) messages. This allows a gateway to move between gatekeepers during the gatekeeper request (GRQ) and registration request (RRQ) phases.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/121/121x/pulclrnt.htm

Ecosystem Gatekeeper Interoperability Enhancements, Phase 2

The H.323 Support for Virtual Interfaces 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.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulgkarj.htm.

Feature Group D Support

This feature extends support for Feature Group D signaling on Cisco platforms. Feature Group D service is a trunk side connection that enables telephone customers to choose their long distance network and use the same number of digits no matter which carrier they use. Routers interface with interexchange carriers using Feature Group D to support voice traffic in the carrier environment.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulhdvfg.htm.

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.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulaltgk.htm.

Gateway-to-Gatekeeper Billing Redundancy

The Gateway-to-Gatekeeper Billing Redundancy feature enhances the accounting capabilities of the Cisco H.323 Gateway and provides support for Vocaltec Gatekeepers. The Gateway-to-Gatekeeper Billing Redundancy feature provides redundant billing information to an alternate gatekeeper if the primary Gatekeeper to which a Gateway is registered becomes unavailable.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulgwgkb.htm.

H.323 Enhancements

This feature consists of the following:

- Source Call Signal Address, which is an enhancement to the admissions request (ARQ) message to allow a source call-signal address field.
- H.245 Empty Capabilities Set, which is a mandatory part of H.323, Version 2. It is used by applications to redirect the voice media stream, which is a new address

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_fts.htm.

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 include in the H.323 packet is deterministic and consistently indicates the same address for the source.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_bnd.htm.

H.323 Version 2 Support

Cisco H.323 Version 2 Support upgrades Cisco IOS software to comply with the mandatory requirements and several of the optional features of the version 2 specification. This upgrade enhances the existing Voice Over IP Gateway, the Multimedia Conference Manager (Gatekeeper and Proxy).

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pullh323.htm.

Interactive Voice Response for Cisco Access Platforms

The Interactive Voice Response (IVR) feature allows the use of one of several interactive voice response scripts during the call processing. The TCL scripts are designed to interact with the IVR application software to perform the various functions. TCL scripts contain both executable files and audio files that interact with the system software. The IVR application is used for information gathering and processing purposes, such as accounting and billing.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_ivr.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 systems provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as an account number. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection), forwards the collected digits to a server for storage and retrieval, and then places the call to the destination phone or system. Call records can be kept and a variety of accounting functions performed.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pullskyn.htm.

Interworking Signaling Enhancements for H.323 VoIP

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables VoIP networks to properly signal the setup and tear-down of calls, including generating in-band tones and announcements when needed at the originating or terminating switch. When a tone (for example, ringback, busy, reorder) or announcement (for example, "The number you have dialed is no longer in service") is played at the destination switch, the backward voice path from the called party to the calling party is cut-through early, so that the calling party can hear the tone or announcement. To prevent fraudulent calls, the voice path is cut-through in both directions only after the Connect message is received from the destination. The call progress indicator, which signals the availability of in-band communication, is carried end-to-end as required when interworking with ISDN and CAS protocols.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pul323pi.htm.

ISDN Network Side for ETSI Net5 PRI

The ISDN Network Side for ETSI Net5 PRI feature enables Cisco IOS to replicate the public switched network interface to a PBX that is compatible with the ETSI Net5 switch type.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtpri.htm.

Monitoring Voice and Fax Services on the Cisco AS5350 and Cisco AS5400 Universal Gateways

The universal port dial feature card (DFC) is a hardware card that processes voice and data services port technology for the Cisco AS5350 and Cisco AS5400. The ports on the Universal Port DFC support multiple types of service including modem, digital, voice, and fax. Ports can be aggregated at the slot level of the Universal Port module, the Service Processing Element (SPE) level within the Universal Port module, and the individual port level.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftupspe.htm.

NTT PRI NFAS

This feature adds the NTT switch type to the existing NFAS with D Channel Backup feature.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtnfas_n.htm

Prepaid Distributed Calling Card via Packet Telephony

The Debit Card for Packet Telephony on Cisco Access Platforms is an application supported by the Cisco Interactive Voice Response (IVR) feature. The IVR voice scripts have been modified to use Tool Command Language (TCL) scripts.

The feature components consist of IVR functionality in Cisco IOS software that work in conjunction with an integrated third-party billing system. The Debit Card feature includes the ability to maintain per-user credit balance information through the use of a billing system. When these features are implemented, the billing system and IOS software functions enable a carrier to authorize voice calls and debit individual user accounts in real time at the edges of a voice-over-IP network, without requiring external service nodes. This feature uses vendor specific attributes (VSAs) to communicate with the billing system.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull0134.htm.

Redundant Link Manager (RLM)

The goal of Redundant Link Manager (RLM) is to primarily provide a virtual link management over multiple IP networks so that the Q.931 signaling protocol and other proprietary protocols can be transported on top of multiple redundant links between the Cisco Signaling Controller (CSC) and the Network Access Server (NAS). In addition to this, RLM opens, maintains, and closes multiple links, manages buffers of queued signaling messages, and monitors whether links are active for link failover and Signaling Controller failover. The user can create more than one IP connection between the CSC and the NAS.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_rlm.htm.

Service Provider Features for Voice over IP

The Cisco voice Service Provider features include enhancements made to the functionality and configuration of both the gateway and the Voice over IP (VoIP) gatekeeper. The architecture of these features provides the Quality of Service (QoS), stability, and functionality necessary for carrier class, real-time IP communications services.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pulvoip1.htm.

Settlement for Packet Voice, Phase 2

The Settlements for Packet Voice, Phase 2 feature contains two features that were not in the first Cisco implementation of OSP (Settlement for Packet Telephony on Cisco Access Platforms): Roaming and PKI Multiple Roots.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pul0123b.htm.

SIP Diversion Header Implementation for Redirecting Number (CSCdr72341)

The SIP Diversion Header Implementation for Redirecting Number feature provides support for a new SIP header field; Call Control (CC)-Diversion. The CC-Diversion header field enables the SIP gateway to pass call control redirecting information during the call setup. Call control redirection is the redirection of a call based on a subscriber service such as call forwarding. Call redirection information is typically used for Unified Messaging and voice mail services to identify the recipient of a message. Call control redirection information can also be used to support applications such as automatic call distribution and enhanced telephony features such as Do Not Disturb and Caller ID.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/sipcfs/hennigan.htm>.

T.38 Fax for Cisco Universal Gateways

A universal port dial feature card (DFC) is a hardware card that processes digital service port technology for the Cisco AS5400. Ports on the universal port DFC support multiple types of services such as modem, fax, digital data, and voice. The universal port DFC provides multiple port sessions, with each session capable of originating or terminating a session over a DS-0 in PCM format. The number of sessions depends on the port density of the card. You can manage your port connections at the universal port slot level, service processing element (SPE) level, or port level using monitoring and troubleshooting commands. A port is defined as an endpoint on a DFC card through which multiservice tones, voice, and data flow. There are six ports per SPE.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtfax.htm.

Voice over IP Q.SIG Network Transparency

Integration of Q.SIG enables Cisco voice switching services to connect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) that communicate by using the Q.SIG protocol.

The Q.SIG protocol is a variant of ISDN D-channel voice signaling. It is based on the ISDN Q.921 and Q.931 standards and is becoming a worldwide standard for PBX interconnection. By using Q.SIG signaling, the Cisco AS5300 can route incoming voice calls from a private integrated services network exchange (PINX) across a wide-area network (WAN) to a peer Cisco AS5300, which can then transport the signaling and voice packets to a second PINX.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/121/121x/pull0125.htm.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM1

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM1.

New Hardware and Software Features in Cisco IOS Release 12.1(5) XM

There are no new hardware and software features in the Cisco AS5350 for Cisco IOS Release 12.1(5) XM.

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

There are no new hardware features in the Cisco AS5350 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 AS5350 for Cisco IOS Release 12.1(5) T.

AAA Broadcast Accounting

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple authentication, authorization, and accounting (AAA) servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

For further details, please see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt_aaaba.htm

AAA Server Group Deadtimer

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.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtaasge.htm>

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.

Cisco Resource Pool Manager CLID/DNIS Call Discriminator

The Cisco RPM CLID/DNIS Call Discriminator feature lets you specify a list of calling party numbers and/or called party numbers to be rejected for inbound calls. You can implement CLID/DNIS screening by expanding the existing call screening or Cisco RPM call discriminator feature. CLID/DNIS call screening provides an additional way to screen calls based on CLID/DNIS for both local and remote RPM.

For further details, please see

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

Ethernet-like Interfaces MIB and Interfaces Group MIB Enhancements

This feature module documents enhancements made to the Interfaces Group MIB module (IF-MIB) and the addition of the Ethernet-like Interfaces MIB module (ETHERLIKE-MIB) in Cisco IOS Release 12.1(2)T. These MIB enhancements bring the IF-MIB into compliance with RFC2233, and implements support for RFC2665 in the ETHERLIKE-MIB. Additionally, you can now configure SNMP to use either the existing Cisco implementation of linkUp / linkDown traps or the new implementation consistent with Internet Engineering Task Force (IETF) standards. This configuration is achieved through the use of a new Cisco IOS CLI command.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/ifmib2.htm>

Event MIB

The Event MIB provides the ability to monitor Management Information Base (MIB) objects on a local or remote system using SNMP and initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified). When notifications are triggered by events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed.

For further details, please see

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

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.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtigmvp3.htm>.

Individual SNMP Trap Support

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

For further details, please see

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

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.

For further details, please see

<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.

For further details, please see

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

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.

For further details, please see

<http://www.Cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtavail.htm>.

MSDP MIB

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple Protocol Independent Multicast sparse-mode (PIM-SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP (or other MSDP SA originator) runs MSDP over TCP to discover multicast sources in other domains.

For further details, please see

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

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.

For further details, please see

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

NAT—Support of H.323 v2 Call Signaling (FastConnect)

Cisco IOS NAT supports all H.225 and H.245 message types, including FastConnect and Alerting, as part of the H.323 v2 specification.

Previously, NAT only supported H.323 version 1 and that was specific only to the Microsoft NetMeeting application. With this enhancement, any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dth323v2.htm>.

NAT—Support of IP Phone to Cisco CallManager

Cisco IP phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco CallManager (CCM). Messages flow back and forth that include IP address and port information used to identify other IP phone users with which a call can be placed.

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

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

For further details, please see

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

NextPort Port Service Management for the Cisco AS5400 Universal Access Server

The NextPort port service management feature implements digital service port technology for the Cisco AS5400. Ports on the Nextport modem carrier module support both modem and digital services. Ports can be addressed aggregated at the slot level of the Nextport module, the Service Processing Element (SPE) level within the Nextport module, and the individual port level. The Service Processing Element (SPE) is an addressable group of six modems. The Nextport dial feature card is supported by Service Processing Element (SPE) operating software.

Benefits include the following:

- Modem or digital service at the port level resulting in greater flexibility of network configuration
- Addressability at the slot, SPE, or port level resulting in ease and scale of configuration tasks
- Higher port density in the platform resulting in economies of scale
- SPE layer buffers the platform architecture from future changes and advances in port level technology

- Modular architecture with resulting ease and economy of maintenance
- The Nextport architecture is designed to be extended to additional port services and other Cisco access server platforms.

For complete information about NextPort Port Service Management for the Cisco AS5400 Universal Access Server, see the following URL:

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

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 re-enabling of this feature.

For further details, please see

<http://www.Cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5parse.htm>.

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.

For further details, please see

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

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 usernames and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtrattr8.htm>

Setting the Port Threshold for the Trunk Card

The Setting the Port Threshold for the Trunk Card feature allows you to avoid dropped calls by setting a port threshold that must be reached before a trunk card transmitter is enabled. In platforms with a CT3 Dial Feature Card (DFC) and one or more universal port (previously called NextPort) DFCs, the CT3 DFC reaches active state before the universal port DFCs because the universal port DFCs have a more complicated download and initialization process than does the CT3 DFC. When the CT3 DFC becomes active, the central office can route calls to the platform. However, if the universal port DFC modules are not yet active, the calls are dropped due to unavailability of resources. The central office does not attempt to route calls to the failed platform again; even if the universal port DFCs subsequently become active, the platform still does not receive calls.

For further details, please see

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

VoIP Call Admission Control Using RSVP

RSVP is the IP service that allows applications to request end-to-end QoS guarantees from the network. Cisco VoIP applications use RSVP for call admission control, limiting the accepted voice load on the IP network to guarantee the QoS levels of calls. The VoIP Call Admission Control using RSVP feature synchronizes RSVP signaling with H.323 Version 2 signaling to ensure that the bandwidth reservation is established in both directions before a call moves to the alerting phase (ringing). This ensures that the called party phone rings only after the resources for the call have been reserved. Using RSVP-based admission control, VoIP applications can reserve network bandwidth and react appropriately if bandwidth reservation fails.

For further details, please see

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt4trsvp.htm>.

WCCP Redirection on Inbound Interfaces

The WCCP Redirection on Inbound Interfaces feature adds support to Cisco IOS software for the redirection of Web Cache Communication Protocol (WCCP) traffic on inbound interfaces. Prior to this release, WCCP could be configured to redirect traffic at an outbound interface only.

This feature offers better redirection performance as well as providing more flexibility in configuring WCCP.

For further details, please see

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

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Deprecated and Replacement MIBs

Old Cisco 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 network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 4](#).

Table 4 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
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 determined
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 determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Limitations and Restrictions

The MICA and microcom modems are not supported on the Cisco AS5350. Only modem, digital, and voice services are supported by using the universal port dial feature card.

Caveats for Cisco IOS Release 12.1 XM

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.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.1 and Cisco IOS Release 12.1 T are also in Cisco IOS Release 12.1(5) XM8.

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

Caveat numbers and brief descriptions of caveats in Cisco IOS Release 12.1(5) XM8 are listed in [Table 5](#) and [Table 6](#). For details about a particular caveat, go to Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the [“Cisco IOS Software Documentation Set”](#) section on page 30.



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, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Open Caveats — Cisco IOS Release 12.1(5) XM8

All the caveats listed in [Table 5](#) are open in Cisco IOS Release 12.1(5) XM8. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 5 Open Caveats for Release 12.1(5) XM8

Caveat ID Number	Description
CSCdv68388	Enhancements/Fixes to Cache Error Exception Handler

Resolved Caveats — Cisco IOS Release 12.1(5) XM8

All the caveats listed in [Table 6](#) are resolved in Cisco IOS Release 12.1(5) XM8. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 *Resolved Caveats for Release 12.1(5) XM8*

Caveat ID Number	Description
CSCdu69834	<code>ip mtu adjust</code> should default to off
CSCdt67753	Need knob to disable automatic MTU adjustment added via CSCdr01713

Open Caveats — Cisco IOS Release 12.1(5) XM7

There are no open caveats specific to Cisco IOS Release 12.1(5) XM7 that require documentation in the release notes.

Resolved Caveats — Cisco IOS Release 12.1(5) XM7

All the caveats listed in [Table 7](#) are resolved in Cisco IOS Release 12.1(5) XM7. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 *Resolved Caveats for Release 12.1(5) XM7*

Caveat ID Number	Description
CSCdw65903	An error can occur with management protocol processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Cisco IOS Release 12.1(5) XM6

All the caveats listed in [Table 8](#) are resolved in Cisco IOS Release 12.1(5) XM5. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 *Open Caveats for Release 12.1(5) XM6*

Caveat ID Number	Description
CSCdv83040	RADIUS attribute 242 does not support protocol 50 and 51

Resolved Caveats—Cisco IOS Release 12.1(5) XM6

All the caveats listed in [Table 9](#) are resolved in Cisco IOS Release 12.1(5) XM6. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Resolved Caveats for Release 12.1(5) XM6

Caveat ID Number	Description
CSCdr08256	* is converted to 0 in the running config
CSCdv48261	improvements to dynamic acls for ios fw
CSCdv45035	Memory leak on 5300/5800 running ThunderVoice
CSCdu81936	Received gratuitous ARP overwrites interface MAC address in ARP tbl
CSCdv75228	Unable to make outbound modem calls or use modemcap after voice call
CSCdv73152	Characters Tx is always 0

Open Caveats—Cisco IOS Release 12.1(5) XM5

There are no open caveats specific to Cisco IOS Release 12.1(5) XM5 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM5

All the caveats listed in [Table 10](#) are resolved in Cisco IOS Release 12.1(5) XM5. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Resolved Caveats for Release 12.1(5) XM5

Caveat ID Number	Description
CSCdt09214	Spurious memory access at vp_ipfib_fixup+0x20

Open Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 11](#) are open in Cisco IOS Release 12.1(5) XM4. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 11 Open Caveats for Release 12.1(5) XM4

Caveat ID Number	Description
CSCdt61467	Need a way to change the default value of VPDN parameters

Resolved Caveats—Cisco IOS Release 12.1(5) XM4

All the caveats listed in [Table 12](#) are resolved in Cisco IOS Release 12.1(5) XM4. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 12 Closed and Resolved Caveats for Release 12.1(5) XM4

Caveat ID Number	Description
CSCds14059	Support for untagged Radius tunnel attributes (attr.69 et al)
CSCds55510	Memory Leak with AAA route download
CSCds63993	H323 GW: IP calls dangling when delay TCP connection occurs
CSCds65611	All B-chan out of serv after controller no-shut then serial no-shut
CSCds71291	Spurious Accesses in mlp_timer
CSCdt11503	IOS crashes when large OID (>256 fields) is received
CSCdt41888	Add dlcx functionality as hidden command
CSCdt46181	Redzone corruption in pptp_tcp_readf()
CSCdt63518	FIB-4-PUNTINTF msg for L2F/MP bundle member w no ip route-cache cef
CSCdt69055	B-channels IN_SERVICE after RESTART when L1 is DEACTIVATED
CSCdt89495	24th channel of T1 0 stays busied-out
CSCdt96253	CRC-32 compensation vulnerability
CSCdt96945	Resource threshold information lost on GK after element failure
CSCdu05205	Memory corruption crash
CSCdu05236	Default disabling of parser cache should not be nvgened
CSCdu07504	sh voice dsp causes reload
CSCdu08214	Calltracker MIB returns NULL for userid when DNIS/ANI is not present
CSCdu14000	Traceback at rlm_link_weight_priority_insert_compare after reload
CSCdu25007	clear spe with calls running could have negative effects
CSCdu27780	AS5300 Suspend message not sent on H323 side with fax configured
CSCdu34741	Term GW doesnt disconnect call which arrives after RLM is down
CSCdu42219	Throttle 21 fails to bring up B channels after reboot w/SS7
CSCdu62721	12.1(5)XM4 candidate fails to bring up B-channels

Open Caveats—Cisco IOS Release 12.1(5) XM3

There are no open caveats specific to Cisco IOS Release 12.1(5) XM3 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM3

There are no resolved caveats specific to Cisco IOS Release 12.1(5) XM3 that require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.1(5) XM2

This section documents possible unexpected behavior by Cisco IOS Release 12.1(5)XM2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds81187

When the PPP Password Authentication Protocol (PAP)-password validation fails—that is, when the PPP PAP password is configured incorrectly—a slow memory leak occurs. There is no workaround.

- CSCdt45598

On a Cisco AS5350, if the “Group-Async” interface has the **ip address negotiated** command enabled and the **group-range** command is removed while traffic is passing through the interface, the router reloads.

Workaround: Do not remove the **group-range command** while traffic is passing through the interface.

Alternative workaround: Instead of the **ip address negotiated** command, configure the **ip unnumbered** command on the “Group-Async” interface.

- CSCdt64336

On a Cisco AS5350, if an NP108 card is hot-swapped with an NP60 card, the **group-range** command under the “Group-Async” interface does not change.

Workaround: Reconfigure the “Group-Async” interface.

Resolved Caveats—Cisco IOS Release 12.1(5) XM2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(5) XM2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds04747

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

This caveat is resolved in Cisco IOS Release 12.1(5)XM2.

Open Caveats—Cisco IOS Release 12.1(5) XM1

There are no open caveats specific to Cisco IOS Release 12.1(5) XM1 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM1

There are no resolved caveats specific to Cisco IOS Release 12.1(5) XM1 that require documentation in the release notes.

Open Caveats—Cisco IOS Release 12.1(5) XM

There are no open caveats specific to Cisco IOS Release 12.1(5) XM that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(5) XM

There are no resolved caveats specific to Cisco IOS Release 12.1(5) XM that require documentation in the release notes.

Related Documentation

The following sections describe the documentation available for the Cisco AS5350. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 28](#)
- [Platform-Specific Documents, page 29](#)
- [Feature Modules, page 29](#)
- [Cisco IOS Software Documentation Set, 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: Cisco IOS Software: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes

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

- The “[Caveats for Cisco IOS Release 12.1 XM](#)” section on page 23

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.1 XM](#)” in these release notes, see *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1T*, which contains 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: Cisco IOS Software: Cisco IOS Release 12.1: Release Notes: 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, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

Platform-Specific Documents

These documents are available for the Cisco AS5350 on Cisco.com and the Documentation CD-ROM:

- Hardware Installation Documents for Cisco AS5350
- Configuration Documents for Cisco AS5350
- Regulatory Compliance and Safety Documents for Cisco AS5350

On Cisco.com at:

Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5350

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5350

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1 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: Cisco IOS Software: 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. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

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

On Cisco.com at:

Technical Documents: Cisco IOS Software: 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 Contents

[Table 13](#) lists 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: Cisco IOS Software: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

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

Table 13 Cisco IOS Release 12.1 Documentation Set

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

Table 13 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> • <i>Cisco IOS Software System Error Messages</i> • <i>New Features in 12.1-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.1 T</i> • <i>Release Notes</i> (Release note and caveat documentation for 12.1-based releases and various platforms) 	

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used with the documents listed in the [“Related Documentation”](#) section on page 28.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other 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. (0201R)

Copyright © 2000–2002, Cisco Systems, Inc.
All rights reserved.