Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(11)YU

July 28, 2003

These release notes describe new features and significant software components for the Cisco 1700 series routers that support Cisco IOS Release 12.2 T, up to and including Release 12.2(11)YU1. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on CCO and the Documentation CD.

For a list of the software caveats that apply to Release 12.2(11)YU1, see the "Caveats" and the online *Caveats for Cisco IOS Release 12.2 T* document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD.

Contents

These release notes discuss the following topics:

System Requirements

This section describes the system requirements for Release 12.2(11)YU1 and includes the following sections:

CISCO SYSTEMS

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

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(11)YU1 on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1710	Cisco 1710 IOS IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	IP/IPX/AT/IBM/ FW/IDS PLUS IPSEC 3DES	c1710-bk9no3r2sy-mz	16 MB	48 MB
	Cisco 1710 IOS IP/FW/IDS PLUS IPSEC 3DES	IP/FW/IDS PLUS IPSEC 3DES	c1710-k9o3sy-mz	8 MB	48 MB
Cisco 1751 and Cisco 1760	Cisco 1700 IOS IP ADSL/IPX/ AT/IBM/VOX/FW/IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/VOX/FW/ IDS IPSEC 56	c1700-bk8no3r2sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/VOX/FW/ IDS PLUS IPSEC 3DES	IP ADSL/IPX/ AT/IBM/VOX/FW/ IDS IPSEC 3DES	c1700-bk9no3r2sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 56	IP/ADSL/ VOX/FW/IDS PLUS IPSEC 56	c1700-k8o3sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX PLUS IPSEC 56	IP/ADSL/VOX PLUS IPSEC 56	c1700-k8sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/VOX/FW/ IDS PLUS IPSEC 3DES	c1700-k9o3sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX PLUS IPSEC 3DES	IP/ADSL/VOX PLUS IPSEC 3DES	c1700-k9sv8y7-mz	16 MB	96 MB
	Cisco 1700 IOS IP/ADSL/IPX/VOX/FW/IDS PLUS	IP/ADSL/IPX/ VOX/FW/IDS PLUS	c1700-no3sv8y7-mz	16 MB	64 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1751 and Cisco 1760	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS	IP/ADSL/VOX/ FW/IDS PLUS	c1700-o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOX PLUS	IP/ADSL/VOX PLUS	c1700-sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP ADSL/IPX/ AT/IBM/VOICE/FW/IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/VOICE/ FW/ IDS IPSEC 56	c1700-bk8no3r2sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/VOICE/ FW/IDS PLUSIPSEC 3DES	IP ADSL/IPX/ AT/IBM/VOICE/ FW/IDS IPSEC 3DES	c1700-bk9no3r2sv3y7-mz	16 MB	64 MB
Cisco 1750/ and Cisco 1760	Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS IPSEC 56	IP/ADSL/ VOICE/FW/IDS PLUS IPSEC 56	c1700-k8o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 56	IP/ADSL/VOICE PLUS IPSEC 56	c1700-k8sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS IPSEC 3DES	IP/ADSL/ VOICE/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES	IP/ADSL/VOICE PLUS IPSEC 3DES	c1700-k9sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/IPX/VOICE/FW/IDS PLUS	IP/ADSL/IPX/ VOICE/FW/IDS PLUS	c1700-no3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS	IP/ADSL/ VOICE/FW/IDS PLUS	c1700-o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/VOICE PLUS	IP/VOICE PLUS	c1700-sv3y-mz	16 MB	48 MB
	Cisco 1700 IOS IP/ADSL/VOICE PLUS	IP/ADSL/VOICE PLUS	c1700-sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/VOX PLUS	IP/VOX PLUS	c1700-sv8y-mz	16 MB	64 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1721/ Cisco 1751 and Cisco 1760	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/FW/IDS PLUS IPSEC 56	c1700-bk8no3r2sy7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	IP ADSL/IPX/ AT/IBM/FW/IDS IPSEC 3DES	c1700-bk9no3r2sy7-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM PLUS	IP /ADSL/IPX/ AT/IBM PLUS	c1700-bnr2sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX/AT/IBM	IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	32 MB
	Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 56	IP/ADSL/FW/IDS PLUS IPSEC 56	c1700-k8o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/ADSL PLUS IPSEC 56	IP/ADSL PLUS IPSEC 56	c1700-k8sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	IP/ADSL PLUS IPSEC 3DES	c1700-k9sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/ADSL/IPX/FW/IDS PLUS	IP/ADSL/IPX/ FW/IDS PLUS	c1700-no3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX	IP/IPX	c1700-ny-mz	8 MB	32 MB
	Cisco 1700 IOS IP/FW/IDS	IP/FW/IDS	c1700-o3y-mz	8 MB	32 MB

Hardware Supported

Cisco IOS Release 12.2(11)YU1 supports the following Cisco 1700 series routers:

- Cisco 1710 routers
- Cisco 1721 routers
- Cisco 1751 and 1751-V routers
- Cisco 1760 and 1760-V routers

The Cisco 1710 and Cisco 1721routers run data images only. The Cisco 1751, 1751-V, 1760, and 1760-V routers run data or data-and-voice images, providing digital and analog voice support.

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers, which are available on Cisco.com and the Documentation CD at the following location: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:
Cisco Product Documentation: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1700 Series Routers**: **<platform_name>**

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 1700 series router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-NY-MZ), Version 12.2(11)YU1, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.2(13.1u)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Software Installation and Upgrade Procedures* located at http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.2(11)YU1 supports the same feature sets as Releases 12.2 and 12.2(8)T, but Release 12.2(11)YU1 includes new features supported by the Cisco 1700 series routers.

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

Table 2 lists the features and feature sets supported in Cisco IOS Release 12.2(11)YU1.

The table 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, "12.2(11)YU" means the feature was introduced in 12.2(11)YU. If a cell in this column is empty, the feature was included in a previous release or the initial base release.

Note These feature set tables only contain a selected list of features, which are cumulative for Release 12.2(11)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set for Cisco 1710 Routers

Feature	In	Feature Set	
		IP/IPX/AT/ IBM/FW/IDS PLUS IPSEC 3DES	IP/FW/IDS PLUS IPSEC 3DES
IPSec			
VPN Device Manager Support	12.2(11)YU	Yes	Yes
AES Support in Cisco IOS Software	12.2(11)YU	Yes	Yes
Look-Ahead Fragmentation	12.2(11)YU	Yes	Yes
IOS Firewall			
SIP Signaling Support	12.2(11)YU	No	No
Websense URL Filtering	12.2(11)YU	Yes	Yes
N2H2 URL Filtering	12.2(11)YU	Yes	Yes
ICMP Stateful Inspection	12.2(11)YU	Yes	Yes
SSL Support for HTTP Authentication Proxy Sign-In	12.2(11)YU	Yes	Yes
IOS IDS			
Signature Enhancement	12.2(11)YU	Yes	Yes
VoIP			
MGCP Support for CallManager	12.2(11)YU	No	No
SNMP			
CISCO-DSP-MGMT-MIB	12.2(11)YU	No	No

Table 3 Feature List by Feature Set for Cisco 1721 Routers

Feature	In	Feature Set				
		IP ADSL/IPX/ AT/IBM/FW/ IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/FW/ IDS IPSEC 3DES	IP/ADSL/ FW/IDS PLUS IPSEC 56	IP/ADSL PLUS IPSEC 56	IP/ADSL/ FW/IDS PLUS IPSEC 3DES
IPSec						
VPN Device Manager Support	12.2(11)YU	Yes	Yes	Yes	Yes	Yes
AES Support in Cisco IOS Software	12.2(11)YU	No	Yes	No	No	Yes
Look-Ahead Fragmentation	12.2(11)YU	Yes	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for Cisco 1721 Routers

Feature	In	Feature Set				
		IP ADSL/IPX/ AT/IBM/FW/ IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/FW/ IDS IPSEC 3DES	IP/ADSL/ FW/IDS PLUS IPSEC 56	IP/ADSL PLUS IPSEC 56	IP/ADSL/ FW/IDS PLUS IPSEC 3DES
IOS Firewall						
SIP Signaling Support	12.2(11)YU	No	No	No	No	No
Websense URL Filtering	12.2(11)YU	Yes	Yes	Yes	No	Yes
N2H2 URL Filtering	12.2(11)YU	Yes	Yes	Yes	No	Yes
ICMP Stateful Inspection	12.2(11)YU	Yes	Yes	Yes	No	Yes
SSL Support for HTTP Authentication Proxy Sign-In	12.2(11)YU	Yes	Yes	Yes	No	Yes
IOS IDS						
Signature Enhancement	12.2(11)YU	Yes	Yes	Yes	No	Yes
VoIP						
MGCP Support for CallManager	12.2(11)YU	No	No	No	No	No
SNMP						
CISCO-DSP-MGMT-MIB	12.2(11)YU	No	No	No	No	No

Table 4, Part 1 Feature List by Feature Set for Cisco 1751 and 1760 Routers

Feature	In	Feature Set					
		IP ADSL/ IPX/AT/ IBM/FW/ IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/ VOX/FW/ IDS IPSEC 3DES	IP/ADSL/ VOX/FW/ IDS PLUS IPSEC 56	IP/ADSL/ VOX PLUS IPSEC 56	IP/ADSL/ VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/ VOX PLUS IPSEC 3DES
IPSec							
VPN Device Manager Support	12.2(11)YU	Yes	Yes	Yes	Yes	Yes	Yes
AES Support in Cisco IOS Software	12.2(11)YU	No	Yes	No	No	Yes	Yes
Look-Ahead Fragmentation	12.2(11)YU	Yes	Yes	Yes	Yes	Yes	Yes
IOS Firewall							
SIP Signaling Support	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes
Websense URL Filtering	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes
N2H2 URL Filtering	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes

Table 4, Part 1 Feature List by Feature Set for Cisco 1751 and 1760 Routers

Feature	In	Feature Set					
		IP ADSL/ IPX/AT/ IBM/FW/ IDS PLUS IPSEC 56	IP ADSL/IPX/ AT/IBM/ VOX/FW/ IDS IPSEC 3DES	IP/ADSL/ VOX/FW/ IDS PLUS IPSEC 56	IP/ADSL/ VOX PLUS IPSEC 56	IP/ADSL/ VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/ VOX PLUS IPSEC 3DES
ICMP Stateful Inspection	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes
SSL Support for HTTP Authentication Proxy Sign-In	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes
IOS IDS							
Signature Enhancement	12.2(11)YU	Yes	Yes	Yes	No	Yes	Yes
VoIP							
MGCP Support for CallManager	12.2(11)YU	No	Yes	No	Yes	Yes	Yes
SNMP							
CISCO-DSP-MGMT-MIB	12.2(11)YU	No	Yes	Yes	Yes	Yes	Yes

Table 4, Part 2 Feature List by Feature Set for Cisco 1751 and 1760 Routers

Feature	In	Feature Set			
		IP/ADSL/ IPX/VOX/ FW/IDS PLUS	IP/ADSL/ VOX/FW/ IDS PLUS	IP ADSL/IPX/ AT/IBM/ VOICE/FW/ IDS IPSEC 56	IP ADSL/IPX/ AT/IBM/ VOICE/FW/ IDS IPSEC 3DES
IPSec					
VPN Device Manager Support	12.2(11)YU	No	No	Yes	Yes
AES Support in Cisco IOS Software	12.2(11)YU	No	No	No	Yes
Look-Ahead Fragmentation	12.2(11)YU	No	No	Yes	Yes
IOS Firewall					
SIP Signaling Support	12.2(11)YU	Yes	Yes	Yes	Yes
Websense URL Filtering	12.2(11)YU	Yes	Yes	Yes	Yes
N2H2 URL Filtering	12.2(11)YU	Yes	Yes	Yes	Yes
ICMP Stateful Inspection	12.2(11)YU	Yes	Yes	Yes	Yes
SSL Support for HTTP Authentication Proxy Sign-In	12.2(11)YU	Yes	Yes	Yes	Yes
IOS IDS					

Table 4, Part 2 Feature List by Feature Set for Cisco 1751 and 1760 Routers

Feature	In	Feature Set			
		IP/ADSL/ IPX/VOX/ FW/IDS PLUS	IP/ADSL/ VOX/FW/ IDS PLUS	IP ADSL/IPX/ AT/IBM/ VOICE/FW/ IDS IPSEC 56	IP ADSL/IPX/ AT/IBM/ VOICE/FW/ IDS IPSEC 3DES
Signature Enhancement	12.2(11)YU	Yes	Yes	Yes	Yes
VoIP					
MGCP Support for CallManager	12.2(11)YU	Yes	Yes	Yes	Yes
SNMP					
CISCO-DSP-MGMT-MIB	12.2(11)YU	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new software features supported by the Cisco 1700 series routers for Release 12.2(11)YU.

New Software Features in Release 12.2(11)YU

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2(11)YU.

VPN Device Manager

Cisco VPN Device Manager (VDM) enables easier Virtual Private Network (VPN) setup and troubleshooting. VDM is used to manage and configure site-to-site VPNs on a single device from a web browser, and to view the effects of configuration changes in real time. VDM implements a wizards-based GUI that allows simplified VPN configuration of the device on which it resides. VDM also monitors general system statistics and router health information such as tunnel throughput and errors. The graphing capability allows comparison of such parameters as traffic volume, tunnel counts, and system utilization.

Advanced Encryption Standard

The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, with cipher block chaining (CBC) mode, to IP Security (IPSec). AES is a privacy transform for IPSec and Internet Key Exchange (IKE) that has been developed to replace the Data Encryption Standard (DES). AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

Pre-fragmentation For IPSec VPNs

When a packet is nearly the size of the maximum transmission unit (MTU) of the outbound link of the encrypting router, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting router reassemble in the process path. Pre-fragmentation for IPSec VPNs increases the decrypting router's performance by enabling it to operate in the high-performance Cisco Express Forwarding (CEF) path instead of the process path.

Pre-fragmentation for IPSec VPNs enables an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the MTU of the output interface, the packet is fragmented before encryption. This avoids process-level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

Firewall Support for SIP

Cisco IOS firewalls identify the source and destination IP address of a message and allow or block the passage of the message according to the configured firewall policy. Firewalls are configured with strict rules specifying static ports through which desirable data can pass while undesirable data is blocked. Messages sent with the Session Initiation Protocol (SIP) contain embedded transport addresses and dynamically allocated port numbers that the firewall cannot access. Embedded IP addresses disrupt signaling when NAT is turned on in conjunction with the IOS firewall. This feature adds support for SIP traffic traversing IOS firewalls on the Cisco 1700 platforms.

Firewall Websense URL Filtering

Websense is a third-party URL filtering software program that can filter Hypertext Transfer Protocol (HTTP) requests, based on destination host name, destination IP address, keywords and username. Websense maintains an URL database of more than 20 million sites organized into more than 60 categories and subcategories. This feature enables the Cisco IOS firewall on the Cisco 1700 router, to do URL filtering based on Websense server. When a Cisco 1700 router receives a HTTP request, it sends a query request to the Websense server with the requested URL. The Websense server does some necessary lookups for the URL and sends back a query response. Based on the Websense server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

Firewall N2H2 Support

N2H2 is globally deployed third-party URL filtering software that can filter HTTP requests, based on destination host name, destination IP address and username and password. It relies on a sophisticated URL database of more than 15 million sites organized into more than 40 categories using both Internet technology and human review. This feature enables the Cisco IOS firewall on the Cisco 1700 router to do URL filtering based on N2H2 server. When a Cisco 1700 router receives a HTTP request, it will send a query request to N2H2 server with the requested URL. N2H2 server does some necessary lookups for the URL and sends back a query response. Based on N2H2 server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceed with normal HTTP processing.

Firewall Stateful Inspection of ICMP

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets reporting errors and other information regarding IP packet processing back to the source. This feature adds support for allowing ICMP traffic (ping and tracroute) originating from the Cisco IOS firewalls configured on a Cisco 1700 router, while denying other ICMP traffic.

Firewall Support of SSL Encrypted HTTP Authentication Proxy Sign-on

The Cisco IOS firewall on the Cisco 1700 router has an application called *authentication proxy* which allows network administrators to apply specific security policies on a per-user basis. When authentication proxy is enabled on the Cisco 1700 router, users can log in to the network or access the Internet via HTTP. This feature adds Secure Socket Layer (SSL)–based encryption support for the user ID and password exchange between the HTTP client and the Cisco 1700 router, when the Cisco IOS firewall authentication proxy is enabled.

Firewall Intrusion Detection System Signature Enhancements

In this release, several new Intrusion Detection System (IDS) signatures have been added to enhance the intrusion detection support, on the Cisco 1700 routers, against Tear Drop, Land Attack, Source Route Filter Option, Java, exe, activeX, Zip, and port scanning types of attacks.

MGCP Support for CallManager (IP-PBX)

The Media Gateway Control Protocol (MGCP) Support for CallManager (IP-PBX) feature enables the Cisco 1751 and Cisco 1760 IOS software to interact with Cisco Call Manager using MGCP. It provides MGCP-based supplementary services, failover, redundancy, and multicast music on hold (MoH) support for CallManager.

CISCO-DSP-MGMT-MIB

The CISCO-DSP-MGMT-MIB monitors the digital signal processing (DSP) resources and status.

New Software Features in Release 12.2(11)T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on CCO:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Service & Support: **Technical Documents**: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cross-Platform Release Notes (Cisco IOS Release 12.2T)**

Limitations

The following sections describe limitations of the new software features supported by the Cisco 1700 series routers for Release 12.2(11)YU1.

Advanced Encryption Standard

Advanced Encryption Standard (AES) cannot encrypt IPSec and IKE traffic if an acceleration card is present and enabled. AES is available in software only.

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Release 12.2 T are also in Release 12.2(11)YU1. For information on caveats in Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document. For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. These documents list severity 1 and 2 caveats, and are located on CCO and the Documentation CD.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in toCisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Release 12.2(11)YU1

Cisco IOS Release 12.2(11)YU1 is a rebuild release for Cisco IOS Release 12.2(11)YU. This section describes unexpected behavior that is fixed in Release 12.2(11)YU1.

Miscellaneous

CSCdz71127

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

CSCea02355

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the

input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Open Caveats for Release 12.2(11)YU

Miscellaneous

CSCdz12275

IPSEC connection fails on Layer3 VPN.

Workaround

Clear the SA, and ping 200 packets twice.

CSCdz10350

ICMP timestamp does not work with NAT overload.

CSCdz17977

cikeGlobalPreviousTunnels gives an incorrect value.

Workaround

No workaround is available.

CSCdz01784

cipSecTunLifeSize gives an incorrect value.

CSCdz03812

“IA exists” is not seen once each minute in Syslog message.

CSCdz02802

DEVCTL_NVRAM_GETVAR devctl does not check for return value.

CSCdz29171

Ping fails for the redundant router ted crypto test.

CSCdz16242

IKE/IPSec SAs get cleared when IPSec idle-timer expires.

CSCdz20150

NAT-T: GRE with flow or CEF switching; counter validation fails.

Workaround

No workaround is available.

CSCdz29619

IKE SA fails, and tunnels fail to come up after failover.

CSCdz06573

SIP: 200 OK of BYE does not pass through with inside static NAT configurations.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. Typically, 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.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(11)YU1. They are located on Cisco.com and the Documentation CD (under the heading **Service & Support**):

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T**

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  Technical Documents: **Product Bulletins**

- To reach the *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in toCisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1700 Series Routers: <platform_name>

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
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 online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

partnership relationship between Cisco and any other company. (0711R)