



Cisco IOS Software Release 12.2(8)YJ

Introduction:

This product bulletin describes the new features introduced in Cisco IOS® Software Release 12.2(8)YJ.

New Features

T1/E1 Multiflex Voice/WAN Interface Cards for Cisco 1721

With this release, the following T1/E1 Multiflex voice interface cards (VWICs) are introduced onto the Cisco 1721 modular router platform.

VWIC-1MFT-E1
VWIC-2MFT-E1
VWIC-1MFT-T1
VWIC-2MFT-T1
VWIC-1MFT-G703
VWIC-2MFT-G703
VWIC-2MFT-T1-DI
VWIC-2MFT-E1-DI

These cards are supported on Cisco 1751, Cisco 1760, Cisco 2600, and Cisco 3600 routers running Cisco IOS Software versions earlier than 12.2(8)YJ.

T1/E1 multiflexi cards, provide the following new data services on the Cisco 1721 in the basic IP images:

- Fractional T1/E1 data service
- Support for two channel groups per module
- Local two ports T1/E1 Drop and Insert service
- E1 Structured (G.704) and Unstructured (G.703) service
- Support 56 Kbps data services

Important Notes

With this release, the services listed above, which are in data-only mode, are supported in Cisco 1700 IOS IP images. They are no longer required in Cisco 1700 IOS IP/VOX Plus or above images. However, for channelized voice services on the Cisco 1751 and Cisco 1760 through T1/E1 VWICs, Cisco 1700 IOS IP/VOX Plus and above images are still required.



Cisco Easy VPN Features

Supporting products: Cisco 1710, 1721, 1751, 1760 routers

Description

- Manual Tunnel Control

A new crypto command can be used when manual configuration has been specified in the Easy VPN configuration. This command is useful for example, when tunnel establishment needs to be manually controlled in ISDN links.

The config commands are as follows:

```
crypto ipsec client ezvpn <name>
```

```
    connect {[auto] | manual}
```

```
crypto ipsec client connect <name> -
```

Config commands:

connect {[auto] | manual} The command has two connect settings: auto and manual. Auto is the default and will automatically attempt to establish a tunnel connection when this config is attached to an interface. The manual option requires the “crypto ipsec client connect <name>” to initiate connections.

- Key Garbling for Easy VPN Encrypted Preshared Keys

The pre-shared keys can be displayed in plain text with the router Show config commands in the current versions of Cisco IOS Software. This feature allows a network administrator to encrypt the pre-shared keys.

Example:

Current behavior with the Show config command:

```
group hw-client-groupname key hw-client-password
```

Present behavior of the show config command:

```
group hw-client-groupname key alsjdkasjdkajl
```

- Easy VPN Access Lists

Easy VPN currently uses extended access-lists to configure NAT for client and split modes. It now uses special access lists, specific to Easy VPN, that cannot be configured by a user via the command line interface.

- DHCP Server Enhancements for Prepending Attributes and DNS Proxy Support

When the tunnel is down, an ISP's DNS should be used. When the tunnel is not down, a customer's DNS should be used to resolve DNS requests. Initially in Cisco IOS Software, DHCP server enhancements supported prepending and selective deletion of imported attributes so that DNS and WINS attributes could be set up correctly in the DHCP Server regardless of whether the tunnel was up or down. This feature now uses the DNS proxy feature.



- The DNS proxy feature:

The router acts as a Proxy DNS server. This means that it will receive DNS queries on behalf of the real DNS servers and proxy for user connected to the LAN. This enables the DHCP server to immediately send out the router's own LAN address as DNS server IP address. The router then forwards the DNS queries from local users to real DNS servers after the WAN connection is initiated, and it caches the DNS records in the answers.

- NAT Configuration Restoration when Tunnel down

When the Easy VPN tunnel is down, users lose Internet connectivity. Easy VPN then auto-configures NAT to implement Client Mode and Split Tunneling. NAT configuration in Easy VPN is based on some of the information learned from the Mode Config command. With NAT autoconfiguration the router must be free of any existing NAT configuration. Internet access requires a default NAT configuration, which can result in is a conflict and Easy VPN not functioning correctly. When the tunnel goes down, all automatically configured NAT config information is removed. In addition, some Internet access NAT config information is removed, which results in user loss of Internet access when the tunnel is down. This feature corrects the current behavior by saving any existing Internet access NAT configurations at tunnel creation time and then restoring it when the tunnel goes down, preventing any loss of Internet connectivity.

- ACL Firewall Interoperability with Easy VPN

In current versions of Cisco IOS Software on 1700 platforms configured for Easy VPN, user entered access-lists fail to work. This feature addresses the interoperability issues between ACLs/Firewalls and Easy VPN.

- Peer Hostname Enhancements

The peer in an Easy VPN configuration can be specified as a dotted decimal IP address or hostname. If a hostname is specified, a DNS lookup is done immediately and the IP address is set internally. However, if the DNS entry changes, the current implementation is not flexible enough to support it. This feature modifies the existing behavior by storing the text string of the hostname and uses this information at the time of tunnel connection, to perform a DNS lookup.

- Multiple Inside Interface Support

Easy VPN currently supports just one inside interface, which defaults to Fast Ethernet on Cisco 1700, and to Ethernet on Cisco 800 and Cisco UBR900 platforms. This feature adds support for multiple inside interfaces which can be configurable under command-line interface the mode as follows:

```
interface <interface-name>  
crypto ipsec client ezvpn <name> [[outside] | inside]
```

- Configurable Inside Interface Support

The Easy VPN feature assumes that the remote network resides on Fast Ethernet 0 interface. Because the Cisco 1700 platform has several different WAN interface cards (WICs), this presents a crucial restriction for customers. This feature adds a command that allows network administrators to specify which interfaces will accommodate remote users when they configure the Easy VPN profile.

- Multiple WAN Interface Support

This feature allows the Cisco 1700 router to support multiple WAN interfaces for Easy VPN remote tunnels.

- Support for Cisco Easy VPN Client initiated to co-exist with other VPN Tunnels



This enables network administrators to create and maintain active crypto maps for VPN tunnels that are not created within the Easy VPN configuration. It also enables administrators to define and maintain VPN tunnels with Easy VPN specific tunnels.

- Support for Simultaneous IPSec Client/Server Operation

This feature enables the router to simultaneously act as a Cisco Easy VPN client and VPN server (VPN remote office extensions, also known as a Cisco Unity™ Server) for Cisco VPN software clients.

- Cisco PIX® Firewall Interoperability

In the existing releases of Easy VPN, customers occasionally cannot connect the Easy VPN to a Cisco PIX Firewall, and IPSec security associations fail to initiate between the Easy VPN client and the firewall. When Easy VPN sends a mode configuration request the firewall, the firewall does not return the mode configuration reply. This feature addresses this problem.

Cisco IOS DHCP Secured IP Address Assignment

This feature allows Cisco 1700 routers to avoid IP spoofing in the wireless LAN environment. This feature for the Cisco IOS DHCP server keeps its database in sync with the Address Resolution Protocol (ARP) table so that IP spoofing can be avoided.

The Cisco IOS DHCP server adds an ARP entry to the ARP table for a client when allocating an address that can only be deleted by the Cisco IOS DHCP server when a binding expires. The ARP entry created by the DHCP server should not be overwritten by any unsolicited ARP requests.

Cisco IOS DHCP Accounting, Accounting Start/Stop Messages

This feature addresses the requirements of clients in a public wireless LAN (PWLAN) access network. It allows a network to send an accounting start message when an address is allocated for a client and an accounting stop message when a DHCP lease is terminated. The server receiving the messages can then act on the notification for accounting purposes. For example, an accounting session can be started when an accounting start/stop message is received, or an accounting session can be cleaned up for a particular DHCP client upon lease termination.

Software

Maintenance Support:

Maintenance for these features will be available on future 12.2X special releases until the code is incorporated into the sixth maintenance software release of 12.2T.

Detailed Information:

For more detailed information about the platforms and features of Release 12.2(8)YJ, reference the following document: Release Notes for Cisco 1700 Series Platforms for Cisco IOS Release 12.2(8)YJ:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/1700/rn1700yj.htm>

Life Span:

Cisco IOS Release 12.2(8)YJ will be sold until the sixth maintenance release of Cisco IOS Software 12.2T.



Support:

Cisco IOS Software Release 12.2(8)YJ is supported by the Cisco Systems Product Support Policy found at the following URL:

<http://www.cisco.com/warp/customer/437/27.html>

Image Product Numbers, descriptions and memory requirements are given below:

Table 1 12.2(8)YJ Image List

Software Product Description	Image	Product Code	T1/E1 Multiflexi VVWICs for 1721	Cisco Easy VPN Features	DHCP Secured IP Address Assignment	DHCP Accounting	Flash	DRAM
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/VOICE/FW/ IDS PLUS IPSEC 56	c1700-bk8no3r2sv3y7-mz	S17Q7HVK8-12208YJ	Yes	Yes	Yes	Yes	32MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/VOX/FW/IDS PLUS IPSEC 56	c1700-bk8no3r2sv8y7-mz	S17Q7V8K8-12208YJ	Yes	Yes	Yes	Yes	32MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/FW/IDS PLUS IPSEC 56	c1700-bk8no3r2sy7-mz	S17Q7HK8-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/VOICE/FW/ IDS PLUSIPSEC3DES	c1700-bk9no3r2sv3y7-mz	S17Q7HVK9-12208YJ	Yes	Yes	Yes	Yes	32MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/VOX/FW/IDS PLUS IPSEC 3DES	c1700-bk9no3r2sv8y7-mz	S17Q7V8K9-12208YJ	Yes	Yes	Yes	Yes	32MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	c1700-bk9no3r2sy7-mz	S17Q7HK9-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/ IPX/AT/IBM PLUS	c1700-bnr2sy7-mz	S17Q7P-12208YJ	Yes	No	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/IPX/ AT/IBM	c1700-bnr2y-mz	S17Q-12208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1700 IOS IP/ADSL/ VOICE/FW/IDS PLUS IPSEC 56	c1700-k8o3sv3y7-mz	S17C7HVK8-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/ VOX/FW/IDS PLUS IPSEC 56	c1700-k8o3sv8y7-mz	S17C7V8K8-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/ FW/IDS PLUS IPSEC 56	c1700-k8o3sy7-mz	S17C7HK8-12208YJ	Yes	Yes	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/ADSL/ VOICE PLUS IPSEC 56	c1700-k8sv3y7-mz	S17C7VK8-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/ VOX PLUS IPSEC 56	c1700-k8sv8y7-mz	S17CV8K8-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL PLUS IPSEC 56	c1700-k8sy7-mz	S17C7K8-12208YJ	Yes	Yes	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/ADSL/ VOICE/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sv3y7-mz	S17C7HVK9-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB



Table 1 12.2(8)YJ Image List (Continued)

Software Product Description	Image	Product Code	T1/E1 Multiflexi VWICs for 1721	Cisco Easy VPN Features	DHCP Secured IP Address Assignment	DHCP Accounting	Flash	DRAM
Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sv8y7-mz	S17C7V8K9-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz	S17C7HK9-12208YJ	Yes	Yes	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES	c1700-k9sv3y7-mz	S17C7VK9-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/VOX PLUS IPSEC 3DES	c1700-k9sv8y7-mz	S17CV8K9-12208YJ	Yes	Yes	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL PLUS IPSEC 3DES	c1700-k9sy7-mz	S17C7K9-12208YJ	Yes	Yes	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/ADSL/IPX/VOICE/FW/IDS PLUS	c1700-no3sv3y7-mz	S17B7HPV-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/IPX/VOX/FW/IDS PLUS	c1700-no3sv8y7-mz	S17B7HPV8-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/IPX/FW/IDS PLUS	c1700-no3sy7-mz	S17B7HP-12208YJ	Yes	No	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/IPX	c1700-ny-mz	S17B-12208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS	c1700-o3sv3y7-mz	S17C7HV-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS	c1700-o3sv8y7-mz	S17C7HV8-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/FW/IDS	c1700-o3y-mz	S17CH-12208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1700 IOS IP/VOICE PLUS	c1700-sv3y-mz	S17CVP-12208YJ	Yes	No	Yes	Yes	16MB	48MB
Cisco 1700 IOS IP/ADSL/VOICE PLUS	c1700-sv3y7-mz	S17C7VP-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/VOX PLUS	c1700-sv8y-mz	S17CV8P-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP/ADSL/VOX PLUS	c1700-sv8y7-mz	S17C7V8P-12208YJ	Yes	No	Yes	Yes	16MB	64MB
Cisco 1700 IOS IP PLUS	c1700-sy-mz	S17CP-1208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1700 IOS IP/ADSL PLUS	c1700-sy7-mz	S17C7P-12208YJ	Yes	No	Yes	Yes	8MB	48MB
Cisco 1700 IOS IP	c1700-y-mz	S17C-12208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1700 IOS IP/ADSL	c1700-y7-mz	S17C7-12208YJ	Yes	No	Yes	Yes	8MB	32MB
Cisco 1710 IOS IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	c1710-bk9no3r2sy-mz	S171QHK9-12208YJ	Yes	Yes	Yes	Yes	16MB	48MB
Cisco 1710 IOS IP/FW/IDS PLUS IPSEC 3DES	c1710-k9o3sy-mz	S171CHK2-12208YJ	Yes	Yes	Yes	Yes	8MB	48MB

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, 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, Fast Step, 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.
(0203R) 06/02 LDI-4039ms 8/8/02