Release Notes for the Cisco 800 and SOHO 90 Series Routers for Cisco IOS Release 12.2(13)ZG

April 7, 2003

These release notes describe new features and significant software components for the Cisco 831, 836, 837 routers and the Cisco SOHO 91, 96 and 97 routers that support Cisco IOS Release 12.2 T, up to and including Release 12.2(13)ZG. 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 Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Release 12.2(13)ZG, see the section "Caveats" and refer to 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.com and the Documentation CD.

Contents

These release notes discuss the following topics:

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

System Requirements

This section describes the system requirements for Release 12.2(13)ZG and includes the following sections:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 3
- Upgrading to a New Software Release, page 3
- Feature Set Tables, page 3

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(13)ZG on the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 routers.

Table 1 Recommended Memory for the Cisco 831, Cisco 836, and Cisco 837, SOHO 91, SOHO 96, and SOHO 97 Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 831	Cisco 831 Series IOS IP/FW IPSec 3DES	IP/FW/IPSec 3DES	c831-k9o3y6-mz	8 MB	32 MB
	Cisco 831 Series IOS IP/FW Plus IPSec 3DES	IP Plus/FW/IPSec 3DES	c831-k9o3sy6-mz	8 MB	32 MB
Cisco 836	Cisco 836 Series IOS IP/FW IPSec 3DES	IP/FW/IPSec 3DES	c836-k9o3y6-mz	8 MB	32 MB
	Cisco 836 Series IOS IP/FW Plus IPSec 3DES	IP Plus/FW/IPSec 3DES	c836-k9o3sy6-mz	8 MB	32 MB
	Cisco 836 Series IOS IP/FW/Dial Backup Plus IPSec 3DES	IP Plus/FW/Dial Backup IPSec 3DES	c836-k9o3s8y6-mz	8 MB	32 MB
Cisco 837	Cisco 837 Series IOS IP/FW IPSec 3DES	IP/FW/IPSec 3DES	c837-k9o3y6-mz	8 MB	32 MB
	Cisco 837 Series IOS IP/FW Plus IPSec 3DES	IP Plus/FW/IPSec 3DES	c837-k9o3sy6-mz	8 MB	32 MB
Cisco SOHO 91	Cisco SOHO 91 Series IOS IP/FW/IPSec 3DES	IP/FW/IPSec 3DES	soho91-k9oy6-mz	8 MB	32 MB
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/IPSec 3DES	IP/FW/IPSec 3DES	soho96-k9oy1-mz	8 MB	32 MB
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW/IPSec 3DES	IP/FW/IPSec 3DES	soho97-k9oy1-mz	8 MB	32 MB

Hardware Supported

Cisco IOS Release 12.2(13)ZG supports the following routers:

- Cisco 831 router
- Cisco 836 router
- Cisco 837 router
- Cisco SOHO 91 router
- Cisco SOHO 96 router
- Cisco SOHO 97 router

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 6. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 831, 836, 837 routers and the Cisco SOHO 91, 96 and 97 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_fix/800/index.htm

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

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Access**: **Cisco 800 Series Routers**: **<platform_name>**

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 831, 836, and 837 routers and Cisco SOHO 91, 96, and 97 routers, 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) C836 Software (C836-K9O3SY6-M), Version 12.2(13)ZG, 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*, which are 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(13)ZG supports the same feature sets as Releases 12.2 and 12.2(8)T, but Release 12.2(13)ZG includes new features supported by the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 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 will likely 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 through Table 4 list the features and feature sets that are supported in Cisco IOS Release 12.2(13)ZG.

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(13)ZG" means that the feature was introduced in 12.2(13)ZG. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.

Note These feature set tables contain only a selected list of features, which are cumulative for Release 12.2(8)*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 831 and Cisco 837 Routers

		Feature Set	
Feature	**In**	**IP/FW/IPSec 3DES**	**IP Plus/ FW/IPSec 3DES**
IPSec NAT Transparency	12.2(13)ZG	Yes	Yes
Pre-Fragmentation for IPSec VPNs	12.2(13)ZG	Yes	Yes
Firewall Intrusion Detection System (IDS) Signature Enhancements	12.2(13)ZG	Yes	Yes
Quality of Service for Virtual Private Networks	12.2(13)ZG	No	Yes
Advanced Encryption Standard	12.2(13)ZG	No	Yes
Firewall Support of Secure HTTP (HTTPS) Authentication Proxy	12.2(13)ZG	Yes	Yes
WCCP Version 2	12.2(13)ZG	No	Yes
Dynamic Multipoint VPN	12.2(13)ZG	No	Yes

Table 3 Feature List by Feature Set for Cisco 836 Router

Feature	In	Feature Set		
		IP/FW/IPSec 3DES	IP Plus/ FW/IPSec 3DES	IP Plus/FW/ Dial Backup IPSec 3DES
IPSec NAT Transparency	12.2(13)ZG	Yes	Yes	Yes
Pre-Fragmentation for IPSec VPNs	12.2(13)ZG	Yes	Yes	Yes
Firewall Intrusion Detection System (IDS) Signature Enhancements	12.2(13)ZG	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	12.2(13)ZG	No	Yes	Yes
Advanced Encryption Standard	12.2(13)ZG	No	Yes	Yes
Firewall Support of Secure HTTP (HTTPS) Authentication Proxy	12.2(13)ZG	Yes	Yes	Yes
WCCP Version 2	12.2(13)ZG	No	Yes	Yes
Dynamic Multipoint VPN	12.2(13)ZG	No	Yes	Yes

Table 4 Feature List by Feature Set for Cisco SOHO 91, SOHO 96, and SOHO 97 Routers

Feature	In	Feature Set
		IP/FW/IPSec 3DES
IPSec NAT Transparency	12.2(13)ZG	Yes
Pre-Fragmentation for IPSec VPNs	12.2(13)ZG	No
Firewall Intrusion Detection System (IDS) Signature Enhancements	12.2(13)ZG	No
Quality of Service for Virtual Private Networks	12.2(13)ZG	No
Advanced Encryption Standard	12.2(13)ZG	No
Firewall Support of Secure HTTP (HTTPS) Authentication Proxy	12.2(13)ZG	No
WCCP Version 2	12.2(13)ZG	No
Dynamic Multipoint VPN	12.2(13)ZG	No

New and Changed Information

The following sections list the new software features supported by the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 routers for Release 12.2(13)ZG.

New Software Features in Release 12.2(13)ZG

The following sections describe the new software features supported by the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 routers for Release 12.2(13)ZG.

IPSec NAT Transparency

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through the Network Address Translation (NAT) or Point Address Translation (PAT) point in the network by addressing many known incompatibilities between NAT and IPSec. This feature encapsulates IPSec packets in a User Datagram Protocol (UDP) wrapper, which allows the packets to travel across NAT devices.

A standard IPSec Virtual Private Network (VPN) tunnel would not work if there are one or more NAT or PAT points in the delivery path of the IPSec packet. This feature makes NAT IPSec aware, thereby allowing remote access users to build IPSec tunnels to home gateways.

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 Intrusion Detection System (IDS) Signature Enhancements

The Cisco IOS Intrusion Detection System (IDS) feature supports intrusion detection technology on all the Cisco IOS–based router platforms when the Cisco IOS firewall is present. The Cisco IOS IDS feature identifies 101 of the most common attacks, using signatures to detect patterns of misuse in network traffic. The Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the IDS signatures. When the Cisco IOS IDS detects suspicious activity, it responds before network security can be compromised, and it logs the event through the Cisco IOS syslog or the Cisco Secure Intrusion Detection System (Cisco Secure IDS, formerly known as NetRanger) Post Office Protocol. The network administrator can configure the IDS system to choose the appropriate response to various threats.

When packets in a session match a signature, the IDS system can be configured to take the following actions:

- Send an alarm to a syslog server or a Cisco Secure IDS Director (centralized management interface)
- Drop the packet
- Reset the TCP connection

Quality of Service for Virtual Private Networks

This feature allows the customer to configure Quality of Service (QoS) features and tunneling/crypto on the same interface.

As VPNs grow to include data, voice, and video traffic, the different types of traffic need to be handled differently in the network. QoS and bandwidth management features allow a VPN to deliver high transmission quality for time-sensitive applications such as voice and video. Each packet is tagged to identify the priority and time sensitivity of its payload, and traffic is sorted and routed based on its delivery priority. Cisco VPN solutions support a wide range of QoS features.

For more details on this feature, refer to the following URL:

http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800b3d15.shtml

Example1

Sample configuration using the Cisco 831 router:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
logging buffered 8000 debugging
no logging console
!
ip subnet-zero
!
ip urlfilter alert
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
request-dialin
protocol pppoe
!
class-map match-all voice
match access-group 102
!
policy-map LLQ
class voice
priority 300
class class-default
fair-queue
policy-map SHAPE
class class-default
shape average 1000000 10000 0
service-policy LLQ
!
```

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
crypto isakmp key 0 1234 address 33.1.1.2
!
crypto ipsec transform-set proposal1 esp-3des
!
crypto map test 10 ipsec-isakmp
set peer 33.1.1.2
set transform-set proposal1
match address 101
qos pre-classify
!
interface Ethernet0
ip address 25.1.1.1 255.255.255.0
hold-queue 100 out
!
interface Ethernet1
no ip address
duplex auto
pppoe enable
service-policy output SHAPE
pppoe-client dial-pool-number 1
!
interface Dialer0
ip address 33.1.1.1 255.255.255.0
ip mtu 1420
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
crypto map test
!
ip classless
ip route 14.0.0.0 255.255.255.0 33.1.1.2
ip route 38.1.1.0 255.255.255.0 33.1.1.2
ip http server
no ip http secure-server
!
access-list 101 permit ip host 25.1.1.5 host 38.1.1.5
access-list 101 permit ip host 25.1.1.4 host 14.0.0.4
access-list 102 permit ip host 25.1.1.4 host 14.0.0.4 precedence critical
access-list 102 permit ip host 14.0.0.4 host 25.1.1.4 precedence critical
!
line con 0
exec-timeout 0 0
no modem enable
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
```

Example2

Sample configuration using the Cisco 837 router:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
logging buffered 8000 debugging
no logging console
!
ip subnet-zero
!
ip urlfilter alert
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
request-dialin
protocol pppoe
!
policy-map pq_policy
class class-default
fair-queue
class voice
priority 200
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
crypto isakmp key 0 1234 address 33.1.1.2
!
crypto ipsec transform-set proposal1 esp-3des
!
crypto map test 11 ipsec-isakmp
set peer 33.1.1.2
set transform-set proposal1
match address 101
qos pre-classify
!
interface Ethernet0
ip address 25.1.1.1 255.255.255.0
no ip route-cache
no ip mroute-cache
load-interval 30
no keepalive
hold-queue 100 out
!
interface ATM0
no ip address
no ip route-cache
no ip mroute-cache
load-interval 30
no atm ilmi-keepalive
dsl operating-mode auto
dsl power-cutback 0
!
interface ATM0.1 point-to-point
```

```
no ip route-cache
no ip mroute-cache
pvc 1/40
vbr-nrt 640 640
tx-ring-limit 3
service-policy output pq_policy
pppoe-client dial-pool-number 1
!
interface Dialer0
ip address 33.1.1.1 255.255.255.0
ip mtu 1492
encapsulation ppp
dialer pool 1
dialer-group 1
crypto map test
!
ip classless
ip route 14.0.0.0 255.255.255.0 33.1.1.2
ip route 38.1.1.0 255.255.255.0 33.1.1.2
ip http server
no ip http secure-server
!
access-list 101 permit ip host 25.1.1.5 host 38.1.1.5
access-list 101 permit ip host 25.1.1.4 host 14.0.0.4
access-list 102 permit ip host 25.1.1.4 host 14.0.0.4 precedence critical
access-list 102 permit ip host 14.0.0.4 host 25.1.1.4 precedence critical
dialer-list 1 protocol ip permit
!
line con 0
exec-timeout 0 0
no modem enable
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end
```

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.

Firewall Support of HTTPS Authentication Proxy

The Firewall Support of HTTPS Authentication Proxy feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data passing between the HTTP client and the Cisco IOS router.

WCCP Version 2

The Web Cache Communication Protocol (WCCP) feature allows you to use a Cisco Cache Engine to handle web traffic, reducing transmission costs and downloading time. This traffic includes user requests to view pages and graphics on WWW servers, whether internal or external to the network, and the replies to those requests. When a user requests a page from a web server (located in the Internet), the router sends the request to a cache engine. If the cache engine has a copy of the requested page in storage, the cache engine sends the user that page. Otherwise, the cache engine retrieves the requested page and the objects on that page from the web server, stores a copy of the page and its objects, and forwards the page and objects to the user.

WCCP transparently redirects HTTP requests from the intended server to a cache engine. End users do not know that the page came from the cache engine rather than the originally requested web server.

WCCP v2 contains the following new features:

- Multiple router support
- Improved security
- Faster throughput
- Redirection of multiple TCP port-destined traffic
- Load distributing applications capability
- Client IP addressing transparency

For more details on WCCP Version 2, refer the following URL:

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/wccp.html

Dynamic Multipoint VPN

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPSecurity (IPSec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP).

Benefits of the DMVPN feature are as follows:

- Hub router configuration reduction
- Automatic IPSec encryption initiation
- Support for dynamically addressed spoke routers
- Dynamic tunnel creation for spoke-to-spoke tunnels

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 Cisco.com:

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 Cisco.com, 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)

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(13)ZG. 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; the documents are located on Cisco.com 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 to Cisco.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.

Open Caveats - Release 12.2(13)ZG

The following sections list the open caveats for the Cisco IOS release 12.2(13)ZG.

CSCea32777

Ping packets (less than 1493 B) are dropped when **pppoe** and **df-bit clear** commands are configured.

Workaround

Use process or Cisco Express Forwarding (CEF) switching.

CSCea32254

WCCP packet redirection fails when **ip wccp web-cache redirect out** command is configured in dialer interface and with CEF enabled.

Workaround

Use **ip wccp web-cache redirect in** command in the inbound interface when using dialer configuration and with CEF enabled.

CSCea31640

WCCP packet return handling—web page is partially downloaded and hangs.

Workaround

Ensure that either CEF or fast switching is enabled on the router interface attached to the cache.

CSCdz78267

Interface command cannot overwrite global command with pre-fragmentation for IPSec VPNs feature.

Workaround

1. Enable the pre-fragmentation for IPSec VPNs feature on global level.
2. Use process switching or CEF switching.

CSCea30398

IDS domain naming system (DNS) signatures 6055, 6056, and 6057 fail.

Workaround

Use dynamic NAT and fast switching.

CSCea44427

Router crashes when **ip wccp version 1** and **ip wccp web-cache** commands are configured.

Workaround

Configure IP address on any interface before configuring **ip wccp version 1** and **ip wccp web-cache** commands.

CSCea27555

WCCP interoperability with HTTP authentication proxy is not successful.

Workaround

Interoperability of WCCP and HTTP authentication proxy is not supported in this release.

CSCea19268

WCCP with multicast address does not work when CEF is enabled.

Workaround

Use one of the following options:

- Enable multicast routing
- Use unicast
- Disable CEF

CSCea25350

Packets greater than 1439 B cannot be sent when pre-fragmentation feature is disabled.

Workaround

Configure **crypto ipsec fragmentation before encryption** command.

CSCea25051

CDP-4-DUPLEX_MISMATCH messages appear with auto/full-duplex configuration.

Workaround

Use one of the following options:

- Enable **no cdp advertise-v2** and **no cdp run** commands.
- Enable **no cdp log mismatch duplex** command.

CSCea45743

Ping rate is 45% when IP CEF is enabled.

Workaround

Do not use IP CEF. Use process switching or fast switching.

CSCea47960

Traceback message appears even without **debug** command enabled.

Workaround

Ignore the traceback message.

Resolved Caveats - Release 12.2(13)ZG

CSCdz71561

New operating multimode support for Annex-B against Lucent digital subscriber line access multiplexer (DSLAM).

The behavior of the *auto* mode of **dsl operating-mode** command has been changed, and two new optional operating modes, *annexb* and *multimode,* are introduced in this release.

Syntax Description

dsl operating-mode [*auto* | *etsi* | *annexb-ur2* | *annexb* | *multimode*]

auto	Autodetect mode
etsi	ETSI mode
annexb-ur2	ITU-T G.992.1 Annex-B mode

annexb	Standard Annex-B mode of ITU-T G.992.1
multimode	Mode chosen by firmware for best operating condition on digital subscriber line (DSL). The final mode at SHOWTIME can be either ETSI mode, or standard Annex-B mode depending on current DSLAM setting.

The *auto* mode will switch between the *multimode* option and the *annexb-ur2* option. After the router is switched on and specified in *auto* mode, the DSL driver will try to set DSL operating mode as *multimode* first. If *multimode* fails, then DSL driver will switch to *annexb-ur2* mode.

The only difference between mode *annexb* and mode *annexb-ur2* is the range of upstream tones used by firmware. All DSLAMs with Annex-B mode line cards should support standard Annex-B mode, that is, *annexb* mode. Both ECI DSLAM and Siemens Sage DSLAM support *annexb-ur2* mode.

The *multimode* option specifies that the firmware has the freedom to select whatever mode is appropriate to the DSL line. In this case, the DSLAM controls which operating mode is used. At the CPE side, asymmetric digital subscriber line (ADSL) firmware just follows the mode set by DSLAM settings. The final mode trained when specified as option *multimode* can be either *etsi* mode or standard *annexb* mode (but not *annexb-ur2* mode). When connecting with Lucent Stinger DSLAM with Annex-B Line card, specifying *multimode* option can achieve the best performance provided by firmware for training at standard *annexb* mode.

Example

To set ADSL operation at standard *annexb* mode, follow the configuration procedure below:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface atm0
Router(config-if)#dsl operating-mode annexb
Router(config-if)#end
Router#
```

To set ADSL operation at *multimode*, follow the configuration procedure below:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface atm0
Router(config-if)#dsl operating-mode multimode
Router(config-if)#end
Router#
```

CSCdz88705

Autodetection of modem/console device on console port.

When backup dial is configured, the router detects whether a modem or console terminal is connected to the console port. When a modem is connected to the console port, the router sends the traffic through the console port to the attached modem. When a console terminal is connected to the console port, the router directs the console session through the console port without user CLI intervention. However, this feature requires that hardware flow control to be configured on the line aux as well line con, as shown below.

Example

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#flowcontrol ?
```

```
NONE Set no flow control
hardware Set hardware flow control
software Set software flow control
Router(config-line)#flowcontrol hardware
Router(config-line)#line aux 0
Router(config-line)#flowcontrol ?
NONE Set no flow control
hardware Set hardware flow control
software Set software flow control
Router(config-line)#flowcontrol hardware
Router(config-line)#sh
line con 0
exec-timeout 0 0
no modem enable
stopbits 1
flowcontrol hardware
line aux 0
stopbits 1
flowcontrol hardware
line vty 0 4
login
```

New CLI command

Under line console configuration, a new CLI is introduced to enable autodetection. Existing **modem enable/ no modem enable** CLI commands will remain as is.

```
Router(config-line)#modem enable autodetect
Router(config-line)#no modem enable autodetect
Router(config-line)#end
```

A new show command **sh line autodetect** will indicate to the user the current detection state (whether a modem or a console has been detected). The Init state indicates that the feature is turned on, but no changes have been detected yet.

```
Router#sh line autodetect
Detection State: Console Attached
Router#sh line autodetect
Detection State: Nothing Attached
Router#sh line autodetect
Detection State: Init State
Router#sh line autodetect
Detection State: Modem Attached
Router#sh line autodetect
Detection State: Feature not enabled
```

CSCdz76392

The Cisco 831 router full-/half- duplex and makefile feature commits.

The Cisco 831 router now supports auto, half, or full duplex operation. Auto duplex is set as default.

Example

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int ethernet1
Router(config-if)#duplex ?
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation
Router(config-if)#duplex auto
Router(config-if)#duplex full
Router(config-if)#duplex half
```

CSCdz71544

Serial number support for ADSL driver.

According to the ITU-T G.992.1 specification, DSLAM can request serial number with 32 bytes in length from CPE router via one of the EOC messages. The Cisco IOS Release 12.2(13)ZG supports serial number returned from CPE router.

The format of serial number is as follows:

- The first 11 B will be the board ID of CPE. See below for details
- There are 5 B unused which follows the first 11 B
- The following one byte indicates if standard Annex-B is used or not, and is used primarily for developer debugging purpose
- The following 3 B indicate digital chip number in Little Endian format
- The following 2 B indicate firmware revision in Little Endian format. For example, firmware revision 4.10.1 will be encoded as 014a in Little Endian and hexadecimal format
- The last 10 B are unused. Value is zero.

The information for the first 11 B will be the same as the board ID displayed when **show version** command is entered. In the following example, the message *JAB05350801* with 11 B in length is same as the first 11B of serial number.

Note With current firmware (version 4.10.1 and above), only those ADSL over ISDN routers (the Cisco 826 and Cisco 836 routers) support serial number feature. For Cisco 837 router, current firmware does not support the serial number feature.

Example1

Example of **show version** command output:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) C836 Software (C836-Y6-M), Version 12.2(13)ZG, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
Synched to technology version 12.2(13.1u)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 27-Mar-03 22:38 by username
Image text-base: 0x800131D8, data-base: 0x806C6D54
ROM: System Bootstrap, Version 12.2(1r)XE2, RELEASE SOFTWARE (fc1)
ROM: C836 Software (C836-Y6-M), Version 12.2(13)ZG, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
Router uptime is 0 minutes
System returned to ROM by reload
Running default software
CISCO C836 (MPC855T) processor (revision 0x1001) with 31744K/1024K bytes of memory.
Processor board ID JAB05350801 (1109164128), with hardware revision 0000
CPU rev number 5
Bridging software.
1 Ethernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
```

```
2048K bytes of processor board Web flash (Read/Write)
Configuration register is 0x0
```

Example2

Example of serial number reading from DSLAM:

```
4a 41 44 30 36 30 39 30 46 59 37 ff ff ff ff ff 0a 46 01 02 01 4a 00 00 00 00 00 00 00 00
00 00
```

- 04a 41 44 30 36 30 39 30 46 59 37

  The first 11 B of ASCII codes in hexadecimal number can be decoded as *JAD06090FY7* which is the board ID.

- ff ff ff ff ff

  Five unused bytes.

- 0a

  This byte identifies if standard upstream tone range is used. In standard Annex-B or ETSI, possible values are *0a* in hexadecimal for 20140 chip set or *0b* in hexadecimal for 20150 chip set. In Annex-B UR2 mode, possible values are *10* in hexadecimal for 20140 chip set or *11* in hexadecimal for 20150 chip set.

- 46 01 02

  These three bytes show that 20140 chip set is used by current CPE. For 20150 chip set, the display values will be 56 01 02.

- 01 4a

  These two bytes show that current firmware version is 4.10.1.

- 00 00 00 00 00 00 00 00 00 00

  The remaining 10 bytes are unused. Value is zero.

Related Documentation

The following sections describe the documentation available for the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 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(13)ZG. 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 to Cisco.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 the Cisco 831, 836, and 837 routers and the Cisco SOHO 91, 96, and 97 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_fix/800/index.htm

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

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Access Routers**: **Cisco 800 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/web/ordering/root/index.html

- 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, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

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.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/index.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.ilmc.com/iq_magazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

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)