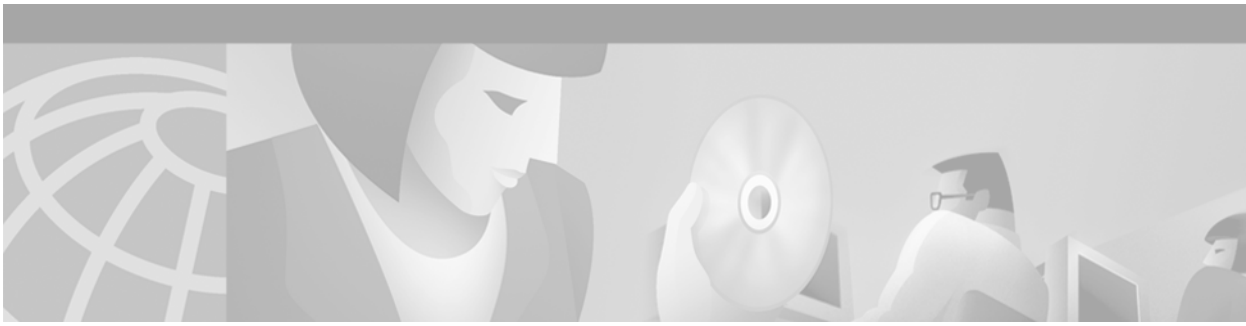

Release Notes for the Cisco 820 Series Routers for Cisco IOS Release 12.2(1)XD

March 25, 2002

These release notes for the Cisco 820 Series Routers describe the enhancements provided in Cisco IOS Release 12.2(1)XD4. These release notes are updated as needed. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM.

For a list of the software caveats that apply to Cisco IOS Release 12.2(1)XD4, see the "Caveats" section on page 12 and *Caveats for Cisco IOS Release 12.2 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Note Cisco IOS Release 12.2(1)XD4 is caveat-to-caveat compatible with Cisco IOS Release 12.1(5)T. Due to last-minute schedule changes, however, Release 12.2(1)XD4 does not contain some of the fixed caveats available in Cisco IOS T-train releases above Release 12.1(5)T.

Contents

These release notes discuss the following topics:

CISCO SYSTEMS

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

78-13221-02

System Requirements

This section describes the system requirements for Release 12.2(1)XD4 and includes the following sections:

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(1)XD4 on Cisco 820 Series Routers.

Table 1 Memory Requirements for the Cisco 820 Series Routers

Platforms	Image Name	Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco 820 Series Routers	Cisco 820 Series IOS IP	c820-y6-mz	8MB	16MB	RAM
	Cisco 820 Series IOS IP/Voice	c820-v6y6-mz	8MB	24MB	RAM
	Cisco 820 Series IOS IP Plus	c820-sy6-mz	8MB	20MB	RAM
	Cisco 820 Series IOS IP/Voice Plus	c820-sv6y6-mz	8MB	24MB	RAM
	Cisco 820 Series IOS IP/FW	c820-oy6-mz	8MB	20MB	RAM
	Cisco 820 Series IOS IP/FW/Voice	c820-ov6y6-mz	8MB	24MB	RAM
	Cisco 820 Series IOS IP/FW Plus IPSec 3DES	c820-k9osy6-mz	8MB	24MB	RAM
	Cisco 820 Series IOS IP/FW/Voice Plus 3DES	c820-k9osv6y6-mz	8MB	32MB	RAM

Hardware Supported

Cisco IOS Release 12.2(1)XD4 supports the following Cisco 820 Series Routers:

- Cisco 826
- Cisco 827 and Cisco 827-4V

For detailed descriptions of new hardware features, see New and Changed Information, page 5.

The Cisco 820 Series Routers provide the following key hardware features:

- The routers provide connection to an ADSL network or telephones and fax machines through an ADSL port.
- Flash memory: Default is 12 MB and is expandable to 20 MB. If 12 MB is Flash is installed, 8 MB is used for the Cisco IOS images and 4 MB hosts the ROMMON and NVRAM. Additional memory can be added using Flash cards.
- Cisco 826 and Cisco 827 Routers Dynamic RAM: Default is 16 MB of DRAM and is expandable to 32 MB.
- Cisco 827-4V Router Dynamic RAM: Default is 24 MB and is expandable to 32 MB. The Cisco 827-4V Router also contains an 8-MB DIMM card.
- The central processing unit is a 50 MHz MPC 855T RISC processor.
- Color-coded ports and cable reduce the chance of cabling errors.
- Routers can be stacked or mounted on a wall.
- The routers provide locking power connectors and a Kensington-compatible locking slot.

Table 2 lists the supported interfaces for the Cisco 820 Series Routers.

Table 2 Supported Interfaces for the Cisco 820 Series Routers

Router	Ethernet Ports	ADSL Ports	Telephone Ports	Console Ports
Cisco 826	One 10BaseT (RJ-45)	RJ-45	–	RJ-45
Cisco 827	One 10BaseT (RJ-45)	RJ-45	–	RJ-45
Cisco 827-4V	One 10BaseT (RJ-45)	RJ-45	Four (RJ-11)	RJ-45

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 820 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) 820 Software (c820-y6-mz), Version 12.2(1)XD4, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For information about upgrading to a new software release, refer to the *Cisco IOS Upgrade Ordering Instructions* product bulletin located at the following URL: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm.

Alternatively, the Cisco IOS Software page on Cisco.com has a variety of information, including upgrade information, organized by release. If you have a Cisco.com account and log in, you can go directly to: http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.

If you have a Cisco.com account and log in, you can reach the new software release upgrade page by going to www.cisco.com and following this path: **Service & Support**: **Software Center**: **Cisco IOS Software**: **Product Bulletins**: **Software**: **General System Software Bulletins**: **Cisco IOS Upgrade Ordering Instructions, No. 957**

You can also reach the Cisco **IOS Upgrade Planner**, which allows you more flexibility to browse for your preferred software, by going to www.cisco.com and following this path: **Service & Support**: **Software Center**: **IOS Upgrade Planner**.

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(1)XD4 supports the same feature sets as Releases 12.2 and 12.2 T, but Release 12.2(1)XD4 can include new features supported by Cisco 820 Series Routers. Table 3 lists the feature sets supported by Cisco 820 Series Routers.

Table 3 Feature Sets Supported by Cisco 820 Series Routers

Image Name	Feature Set Matrix Terms	Software Image	Platform
Cisco 820 Series IOS IP	IP	c820-y6-mz	Cisco 820 Series Routers
Cisco 820 Series IOS IP/Voice	IP/Voice	c820-v6y6-mz	
Cisco 820 Series IOS IP Plus	IP Plus	c820-sy6-mz	
Cisco 820 Series IOS IP/Voice Plus	IP/Voice Plus	c820-sv6y6-mz	
Cisco 820 Series IOS IP/FW	IP/FW	c820-oy6-mz	
Cisco 820 Series IOS IP/FW/Voice	IP/FW/Voice	c820-ov6y6-mz	
Cisco 820 Series IOS IP/FW Plus IPSec 3DES	IP/FW Plus IPSec 3DES	c820-k9osy6-mz	
Cisco 820 Series IOS IP/FW/Voice Plus 3DES	IP/FW/Voice Plus 3DES	c820-k9osv6y6-mz	

Table 4 lists the features and feature sets supported by the Cisco 820 series routers in Cisco IOS Release 12.2(1)XD4.

Each table uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

Note These feature set tables only contain a selected list of features. These tables are not cumulative—nor do they list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 820 Series Routers

	Feature Sets							
Features	**IP**	**IP Plus**	**IP/ FW**	**IP/FW/ Plus/ IPSec/ 3DES**	**IP/Voice**	**IP Voice Plus**	**IP/FW Voice**	**IP/FW/ Voice/ Plus/ IPSec/ 3DES**
Miscellaneous								
DCHP Import	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPCP Subnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SA Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSH	No	Yes	No	Yes	No	Yes	No	Yes
IP Named Access List	No	Yes	No	Yes	No	Yes	No	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco Cisco 820 Series Routers series routers for Release 12.2(1)XD4 and above:

New Hardware Features in Release 12.2(1)XD

Cisco 826 routers connect corporate telecommuters and small offices via Internet Service Providers (ISPs) over asymmetric digital subscriber lines (ADSLs) to corporate LANs and the Internet. The router can provide bridging and multiprotocol routing between LAN and WAN ports. Cisco 826 routers provide connectivity to an ISDN network through an ADSL port.

New Software Features in Release 12.2(1)XD

The following sections list the new software features supported by the Cisco 820 Series Routers for Release 12.2(1)XD. Information is included for any changed or new command line interface (CLI) commands associated with the new features.

DHCP Server Import

The Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server now allows a network administrator to enable Point-to-Point Protocol (PPP) to automatically configure the Domain Name System (DNS) and Windows Internet Name Service (WINS) Server IP address information within a Cisco IOS DHCP Server Pool(s). Enabling this automatic configuration works in conjunction with network access server commands that prevent a peer from receiving a negative acknowledgement (containing addresses for the peer to use), in response to an IP Control Protocol (IPCP) configuration peer request with non-zero addresses in the DNS and WINS options. (WINS is also known as the NetBios Name Server [NBNS].)

Use the following commands to enable PPP to automatically configure the DNS and WINS Server IP address information within a Cisco IOS DHCP Server Pool(s).

- `router(config-if)# ppp ipcp dns {request|reject|A.B.C.D.|accept}`

Command Elements	Description
request	Request server addresses from the peer.
reject	Reject negotiations with the peer.
A.B.C.D.	Primary DNS IP address.
accept	Accept any non-zero DNS address.

- `router(config-if)# ppp ipcp wins {request|reject|A.B.C.D|accept}`

Command Elements	Description
request	Request server addresses from the peer.
reject	Reject negotiations with the peer.
A.B.C.D.	Primary WINS IP address.
accept	Accept any non-zero WINS address.

Note The above commands were introduced on the Cisco 820 Series Routers in Cisco IOS Release 12.2(1)XD.

IPCP Subnet Mask Delivery

Network administrators can assign IP address pools to customer premises equipment (CPE) devices, which, in turn, assign IP addresses to actual CPE and to a DHCP pool. This feature has three requirements:

- The Cisco IOS CPE device must be able to request and use the subnet.
- The Authentication, Authorization, and Accounting (AAA) Radius must be able to both provide that subnet and insert the framed route into the proper Virtual Route Forwarding (VRF) table.
- The provider edge (PE) router must be able to facilitate providing the subnet (via IPCP).

This functionality also exists in a non-Multiprotocol Label Switching (MPLS) environment if the CPE device is a Cisco 600 series router (which does not run Cisco IOS).

Configuring with IPCP Subnet Masks

Perform the following steps to configure your router to use IPCP subnet masks.

Note The commands described in the following steps were introduced on the Cisco 820 Series Routers in Cisco IOS Release 12.2(1)XD.

Step 1 Define an IP DHCP pool *poolname* using the global configuration commands below. For example:

```
Router(config)# ip dhcp pool IPPOOLTEST
Router(dhcp-config)# import all
Router(dhcp-config)# origin ipcp
```

The command **import all** imports the DHCP option parameters. The command **origin ipcp** configures the origin of the pool.

Step 2 Assign the Ethernet interface IP address using the command **ip address pool** *poolname*. For example:

```
Router(config-if)# ip address pool IPPOOLTEST
```

Step 3 Configure the dialer interface in the configuration interface command mode as follows:

a. Assign an IP address:

```
Router(config)# interface Dialer0
Router(config-if)# ip unnumbered Ethernet0
```

b. Set the IPCP negotiation parameters:

```
router(config-if)# ppp ipcp mask {request|reject|A.B.C.D}
```

Command Elements	Description
reject	Reject subnetmask negotiation from the peer.
request	Request the subnet mask from the peer.
A.B.C.D.	Subnet mask to provide to the peer.

The following sample shows a Cisco 827 router configured to use IPCP subnet masks:

```
Router# show run
 Building configuration...

 Current configuration :1479 bytes
 !
 version 12.2
 no service single-slot-reload-enable
 no service pad
 service timestamps debug datetime msec
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router
 !
 no logging buffered
 logging rate-limit console 10 except errors
 !
 username 6400-nrp2 password 0 lab
 ip subnet-zero
 ip dhcp smart-relay
 !
 ip dhcp pool IPPOOLTEST
    import all
    origin ipcp
```

```
!
no ip dhcp-client network-discovery
!
interface Ethernet0
 ip address pool IPPOOLTEST
 ip verify unicast reverse-path
 shutdown
 hold-queue 32 in
!
interface ATM0
 no ip address
 atm ilmi-keepalive
 bundle-enable
 dsl operating-mode auto
 hold-queue 224 in
!
interface ATM0.1 point-to-point
 pvc 1/40
  no ilmi manage
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface Dialer0
 ip unnumbered Ethernet0
 ip verify unicast reverse-path
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname Router
 ppp chap password 7 12150415
 ppp ipcp accept-address
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
dialer-list 1 protocol ip permit
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Service Assurance Agent

The Service Assurance (SA) Agent feature is both a new name for and an enhancement to the Response Time Reporter (RTR) feature introduced in Cisco IOS Release 11.2. The response time and availability monitoring capabilities of RTR now include support for Voice over IP (VoIP), quality of service (QoS), and the World Wide Web.

The SA Agent is an application-aware synthetic operation agent that monitors network performance by measuring key metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, and packet loss. This feature is intended to provide support for Service Level Agreement (SLA) reporting functionality of the Cisco VPN Solution Center, but can also be used for troubleshooting, for analysis before problems occur, and for designing future network topologies. Response Time Monitoring (RTTMON) functionality is supported.

Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS. The SSH server feature enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality similar to an inbound Telnet connection.

The SSH server in Cisco IOS works with publicly and commercially available SSH clients. Before SSH, security was limited to Telnet security. SSH allows strong encryption to be used with Cisco IOS authentication.

Note NOTE: The SSH Client is not implemented.

The SSH has the following restrictions:

- Rivest, Shamir, and Adelman (RSA) authentication available in SSH clients is not supported in the SSH server for Cisco IOS.
- User ID and Password authentication only.
- Supported on DES (56-bit) data encryption and Triple DES (168-bit) data encryption software images only. In the DES (56-bit) software images, DES is the only encryption algorithm available. In the Triple DES software images, both DES and Triple DES encryption are available.

IP Named Access Lists

You can identify IP access lists with an alphanumeric string (a name) rather than a number. Named access lists allow you to configure more IP access lists in a router than using numbered access lists. This feature is required to support the VPN Solution Center, which does not operate with numbered access lists.

New Software Features in Release 12.2(1)

For information regarding the features supported in Cisco IOS Release 12.2, 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/index.htm

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

Service & Support: **Technical Documents**: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Cisco IOS Release 12.2**

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(1)XD4 and above that can apply to the Cisco 820 Series Routers. (Also, see the “Caveats” section on page 12.)

Cisco 820 Series Memory Management When Using WFQ

When weighted fair queuing (WFQ) is used on the Dialer interface, or when WFQ is used in the default class of a service policy, the following parameters need to be set to the values shown because of the limited amount of memory on the router:

- Congestive Discard Threshold: 64 or less
- Number Dynamic Conversation Queues: 64 or less
- Total maximum output packets: 64 or less

For example, if you apply WFQ to the Dialer interface, you need to configure it as follows:

```
interface Dialer 1
 fair-queue 64 64 0
 hold-queue 64 out
```

In this example, the command **fair-queue** *64 64 0* limits the number of conversations to 64, and sets the discard threshold to 64. The command **hold-queue** *64* **out** limits the maximum number of output packets to 64.

In another example, if you configure a service policy, and WFQ is used on the default class, you need to configure the policy as follows:

```
policy-map mypolicy
 class voice
  priority 100
 class class-default
  fair-queue 64
  queue-limit 64

 int dialer 1
 service-policy out mypolicy
 hold-queue 64 out
```

Here, the command **fair-queue** *64* limits the number of conversations to 64, and the command **queue-limit** *64* sets the discard threshold to 64. The command **hold-queue** *64* **out** limits the maximum number of output packets to 64. Failure to configure the above parameters may cause the router to display out-of-memory messages when a large amount of mixed traffic is transmitted from Ethernet to ATM.

Cisco 820 Series Router Clock—CSCdp09409

To run IPSec successfully, the Cisco 820 series router clock needs to be set accurately. Cisco 820 series router clocks are set and maintained using Simple Network Time Protocol (SNTP). For best results, set up a Network Time Protocol (NTP) server to periodically send time information messages to Cisco 820 series routers. See the SNTP configuration and command reference documentation for configuration instructions. If you do not have an NTP server, you must reset the Cisco 820 series router clock using the command **clock set** each time you restart the router.

The SNTP configuration documentation is available in the chapter "Monitoring the Router and Network" volume of the *Configuration Fundamentals Configuration Guide* in the Cisco IOS documentation set. The SNTP command reference documentation is available in the chapter "Router and Network Monitoring Commands" in the "System Management Commands" volume of the *Configuration Fundamentals Command Reference* manual of the Cisco IOS documentation set.

CiscoView Application Support

The CiscoView application supports the Cisco 820 series routers. The CiscoView application provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, concentrators, and adapters. It displays a graphical view of Cisco devices. This network management tool also provides configuring and monitoring functions and offers basic troubleshooting tips.

Downloading Images

Before attempting to download new images, you must first delete files in the router Flash memory. Be sure to use the **delete** command, not command **erase**, to free up space. Entering **erase** removes all files, including the configuration.

Multilink PPP and Interleaving

Multilink PPP fragments large data packets so that small voice packets can be interleaved within them. However, apart from first-in-first-out (FIFO) queuing, no other kind of output queuing mechanisms are currently supported with PPP over ATM. Consequently, when multilink PPP is configured on the Cisco 827 routers, the big packets are fragmented, but interleaving of small voice packets within them does not occur.

NAT Support for H.323 Signaling

Currently, NAT does not support alerting H.225 messages. Therefore, NAT communication cannot be established between the router end points. NAT support for H.323 signaling is limited to the Netmeeting application.

Phone Mate Answering Machine Model 9200

A Phone Mate answering machine model 9200 fails to recognize the ringing signal sent by AMD R79 ringing SLIC. This was confirmed by testing against Phone Mate model 3750 and newer model 9300.

ROM Monitor set stop-bits Parameter

This release supports the setting of 1 only, for the ROM monitor **set stop-bits** parameter.

Caveats

Caveats describe unexpected behavior 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 Cisco IOS Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(1)XD4. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on CCO and the Documentation CD-ROM.

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 - Releases 12.2(1)XD3 and 12.2(1)XD4

This section describes unexpected behavior that is fixed in Releases 12.2(1)XD3 and 12.2(1)XD4.

Management

CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Caveats for Release 12.2(1)XD1

This section describes possibly unexpected behavior by software Release 12.2(1)XD1.

Resolved Caveats for Release 12.2(1)XD1

This section describes possibly unexpected behavior by software releases prior to Release 12.2(1)XD1 that have been resolved in Release 12.2(1)XD1 and above.

CSCdt77246:

When a router is configured for PPPoE and IP NAT, and an incoming packet does not contain an MSS field or its TCP option field is not terminated by 0, the router might stop routing packets. This defect has been fixed in 12.2(1)XD1 release.

Unresolved Caveats for Release 12.2(1)XD1

This section describes possibly unexpected behavior by software Release 12.2(1)XD1.

CSCdt92752

If you remove the current access-list from the encryption map, change the definition of the access-list, and then reassign the access-list to the encryption map, the access-list does not become active. Use the following solutions to work around this problem:

- To change a definition in the current access-list, directly change the access-list definition instead of removing the access-list from the encryption map.
- To assign a different access-list to the encryption map, remove the old access-list from the encryption map, assign the new access-list to the encryption map, and then define the new access-list. For example:

```
crypto map map1 10 ipsec-isa
no match address 100
crypto map map1 10 ipsec-isa
match address 110
no access-list 110
access-list 110 permit ip host 2.0.1.26 host 4.0.1.25
```

CSCdt94260

While using the Dialer interface with Cisco Express Forwarding (CEF) enabled, when you connect a Cisco 820 series router to an access aggregator (such as a Cisco 6400 or Cisco 7200), Unicast Reverse Path Forwarding (URPF) incorrectly drops incoming ping packets from the access aggregator. This problem is caused by the Dialer CEF feature, which is on by default when CEF is enabled. To work around this problem, use the dialer interface command **no ip route-cache cef** to disable the Dialer CEF feature.

CSCdt95764

If you use the DHCP client feature to assign an encryption map to a Bridge Group Virtual Interface (BVI) before the BVI is up or active, the encryption map does not become active and an IPSec tunnel is not built. To work around this problem, assign the encryption map to the BVI again, after the BVI comes up. Note that rebooting the router alone does not fix the problem because the BVI is down before the reboot.

CSCdt98274

The command **ip add dhcp client-id ethernet 0** is available under the BVI but cannot be applied after the DHCP client receives an IP address from the DHCP server. For example, if you enter the command **ip address dhcp** for BVI 1, then enter the command **ip address dhcp client-id e0** on BVI 1 after the Cisco 827 router (the DHCP client) receives an IP address from the DHCP server, and follow up with the command **show run**, the following output is displayed:

```
...   ...   ...   ...   ...
!
 interface BVI1
  ip address dhcp
  crypto map map1
  ...   ...   ...   ...   ...
```

To work around this caveat, delete the existing IP address DHCP by entering the command **no ip address dhcp**. Enter the command **ip address dhcp client-id ethernet 0**, followed by the command **ip address dhcp client-id ethernet 0**.

Similarly, for the BV1 interface, if you enter the command **ip address dhcp client-id ethernet 0** and, after the Cisco 820 Series Router (the DHCP client) receives an IP address from the DHCP server, you enter the command **ip address dhcp** for BVI 1, followed by the command **show run**, the following output is displayed:

```
  ...   ...   ...   ...   ...
!
 interface BVI1
  ip address dhcp client-id ethernet 0
  crypto map map1
  ...   ...   ...   ...   ...
```

To work around this bug, delete the existing IP address by entering the command **no ip address dhcp client-id ethernet 0**, and then issue a new IP address using the command **ip address dhcp**.

CSCdu02130

Cisco 820 series routers unexpectedly reload if you change the tranform set during an active IPSec tunnel and then clear the previous active IPSec tunnel. To work around this problem, clear the active IPSec tunnel before changing the tranform set for the active IPSec tunnel, then reapply the tranform set to the encryption map.

CSCdu02585

Cisco 827 routers do not filter IPSec packets with dynamic maps. This problem occurs when upgrading from a k2 image to a k9 image. For example, the image c820-k2nosy6-mz works properly before an upgrade.

Related Documentation

The following sections describe the documentation available for the Cisco 820 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-ROM.

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

- Release-Specific Documents
- Platform-Specific Documents
- Feature Modules
- Cisco IOS Software Documentation Set

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(1)XD4. They are located on Cisco.com and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.2*
  - To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2* from Cisco.com, click on this path (under the heading **Service & Support**):

    Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**
  - To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2* on the Documentation CD-ROM, click on this path:

    Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**
- Product bulletins, field notices, and other release-specific documents

  To reach these documents from Cisco.com, click on this path (under the heading **Service & Support**):

  Technical Documents: **Product Bulletins**
- *Caveats for Cisco IOS Release 12.2 and 12.2 T*

  The *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents contain caveats applicable to all platforms for all maintenance releases of Release 12.2.
  - To reach the caveats document from Cisco.com, click on this path (under the heading **Service & Support**):

    Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Caveats**
  - To reach the caveats document on the Documentation CD-ROM, click on this path:

    Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS 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

The following documents are available for the Cisco 820 Series Routers on Cisco.com and the Documentation CD-ROM:

Cisco 826 Router

These documents are available for the Cisco 826 router on Cisco.com and the Documentation CD-ROM:

- *Quick Start Guide - Setting up the Cisco 826 Router*
- *Cisco 826 Router Hardware Installation Guide*

- *Software Enhancements for the Cisco 826 and 827 Routers*
- *Regulatory Compliance and Safety Information for the Cisco 826 Router*

Cisco 827 and Cisco 827 4-V Routers

These documents are available for the Cisco 827 and Cisco 827 4-V routers on Cisco.com and the Documentation CD-ROM:

- *Quick Start Guide - Setting Up the Cisco 827 Routers*
- *Cisco 827 Routers Hardware Installation Guide*
- *Cisco 827 Routers Software Configuration Guide*
- *Release Notes for Cisco 827 Routers*
- *Upgrading Memory in Cisco 800 Series Routers*

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**: **Cisco 827 Routers**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**: **Cisco 827 Routers**

Feature Modules

Feature modules describe new features supported by Release 12.2 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

To reach the Release 12.2 feature modules:

- From Cisco.com, click on this path (under the heading **Service & Support**):

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2X Releases**

- From the Documentation CD-ROM, click on this path:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**: **New Features in 12.2-Based Limited Lifetime Releases**: **New Features in 12.2X Releases**

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to set up an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

The Cisco IOS software documentation set is available on Cisco.com and on the Documentation CD-ROM.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Release 12.2 Documentation Set

Table 5 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form.

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

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 5 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • New Features in 12.2-Based Limited Lifetime Releases • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

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

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

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