78-5994-07 01/14/00

Release Notes for Cisco Broadband Operating System Release 2.2.0

January 14, 2000

These release notes discuss primary fixes, new features, important notes, open and resolved caveats, and the software upgrade process for the **Cisco Broadband Operating System (CBOS) Release 2.2.0**. Please refer to previous release notes for specific information concerning past releases.

For more detailed information about the features in these release notes, refer to the "Related Documentation" section on page 20. Information about electronic documentation can be found in the "Cisco Connection Online" section on page 20.

1. Contents

These release notes provide the following information:

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

2. Introduction

CBOS is the common operating system for most of Cisco's customer premises equipment (CPE) products. CBOS is modeled after Cisco's Internetworking Operating System (IOS) and features a similar command syntax and format. This operating system is bundled with the CPE products listed below and can also be downloaded from Cisco Connection Online.

The CBOS Release 2.2.0 supports the following Cisco ADSL CPE products:

- Cisco 675
- Cisco 675e

The CBOS Release 2.2.0 also supports the following Cisco SDSL CPE products:

- Cisco 633

Note The Cisco 633 product does not use all of the feature set of CBOS. When a feature listed in Section 3 does not apply to the Cisco 633, the feature is marked accordingly.

- Cisco 673

3. New Features for the CBOS Release 2.2.0

The **CBOS Software Release 2.2.0** supports the following new features:

3.1 PAT Enhancements

Note The following PAT and NAT features do not apply to the Cisco 633.

CBOS Release 2.2.0 adds Port Address Translation (PAT) enhancements to existing Network Address Translation (NAT) functionality. PAT and NAT enhancements are discussed in the following sections.

3.1.1 NAT support for the XDMCP protocol

CBOS Release 2.2 adds NAT support for (X-Display Manager Client Protocol (XDMCP) used for communications between X-Displays (clients) and X Display Managers (XDM). CBOS does this by translating the XDMCP protocol *Request* message, which embeds display hosts IP address, using NAT. Support for a single Connection Address only is provided in the request message.

The XDMCP protocol uses User Datagram Protocol (UDP) port 177 for messaging between display host and the server host and Transmission Control Protocol (TCP) port 6000, for displaying.

For inside-display-outside-server configurations, a static NAT entry for TCP port 6000 is required. In the case of an outside-display-inside-server configuration a static NAT entry for UDP port 177 is required.

Note Indirect Queries from Displays are not supported.

3.1.2 Support for Wildcard Static NAT entries

CBOS Release 2.2.0 adds support for wildcard static NAT entries. With this feature, you do not have to create one static entry per service port. You can direct all incoming connections to a single inside host irrespective of the port (e.g., File Transfer Protocol (FTP), Telnet, or web interface). This feature is supported in both PPP mode and RFC1483 mode.

NAT Commands Using Wildcards

Previous versions of CBOS required that you explicitly enter the port number and protocol name when adding a static NAT entry. CBOS Release 2.2.0 does not require you to do this. See the following example for more information.

To add a static NAT entry with wildcards for both the port number and protocol name, enter the following:

set nat entry add inside_ipaddress

To add a NAT entry with a wildcard protocol:

set nat entry add inside_ipaddress *portnum*

NAT Commands With No Changes

The following NAT commands have not changed:

Table 1 NAT Commands with No Changes

Command	Description
set nat entry delete all	Deletes all NAT entries.
set nat entry delete inside *inside_ip_address*	Deletes all NAT entries that match the specified inside IP address.
set nat entry delete outside *outside_ip_address*	Deletes all NAT entries that match the specified outside IP address.
show nat	Displays all NAT entries, including static and wildcard Wildcard entries display as asterisks.

You can also override wildcard mapping with a specific mapping for a specific service. To direct different services to different hosts, you can specify a combination of specific NAT entries and wildcard NAT entries. NAT function first looks for a specific NAT entry that matches the port, protocol, and address and if one exists, NAT uses it. Otherwise, NAT uses the wildcard NAT entry.

NAT Commands With Changes

The following table shows the applicable changes in the NAT command syntax:

Table 2 NAT Commands with Changes

Old (Pre-2.2.0) Version of Command	New (2.2. 0 and higher) Version of Command	Description
set nat entry delete *inside_ipaddress portnum outside_ipaddress portnum protocolname*	**set nat entry delete** *inside_ip_address portnum protocolname*	Both entries delete a specific static NAT entry.
set nat entry add *inside_ipaddress* ***portnum*** *outside_ipaddress* ***portnum protocolname***	**set nat entry add** *inside_ipaddress portnum protocolname*	Both entries add a specific static NAT entry.

Note CBOS 2.2.0 supports both versions of the preceding commands. However, Cisco recommends that you use the latest version.

3.1.3 Support for NAT Entries Using IPCP

This feature allows static NAT entries to automatically assume the Internet Protocol Control Protocol (IPCP) address. This means that you no longer have to specify the outside IP address, its port number or its protocol name. IPCP now assigns the outside IP address for translation in the case of PPP routing. In RFC1483 routing mode, the outside IP address has to be manually set.

3.1.4 Support for NAT with VIP Interfaces

CBOS Release 2.2.0 adds support for using NAT with Virtual Interfaces (VIPs) selectively. This feature allows DSL service providers to set up multiple subnets to the CPE and NAT only one of the subnets. This works in the following manner:

- Physical interface ETH0 is configured as inside of the NAT boundary.
- All VIPs (virtual interfaces) and WAN0-0 are treated as outside networks.
- IP traffic between ETH0 and WAN0-0 only is translated when NAT is enabled in CBOS.
- IP traffic between VIP interfaces and other interfaces will not be translated.
- VIPs have to be configured manually whether NAT is enabled or not.

Since VIPs are virtual interfaces on top of ETH0 with the same MAC address, CBOS cannot differentiate ETH0 traffic from VIP traffic without explicitly looking at the IP addresses configured. See the following sections to see how NAT looks at the IP addresses to make this differentiation:

For data received on WAN0-0

If the destination IP address is the NAT inside global IP address, then NAT translates the address in an outside to inside direction. Otherwise, NAT does not translate the traffic.

For data received on ETH0 (including VIPs)

If the source IP address is part of ETH0 configured subnet and the transmit port is the WAN0-0 port, then NAT translates the address in an inside to outside direction. Otherwise, NAT does not translate the traffic.

When NAT is enabled, NAT translates only inside to outside traffic and outside to inside traffic. NAT treats traffic in the following manner:

- Inside to Outside traffic—Route first and translate (NAT) later
- Outside to Inside traffic—Translate (NAT) first and route later.

3.1.5 Support for IGMP Proxy Support with NAT and PAT

CBOS Release 2.2.0 adds Internet Group Management Protocol (IGMP) proxy support with NAT and PAT. This support is mainly for IGMP messages and UDP data destined to multicast destinations. Applications such as IP/TV is be supported only in multicast (scheduled broadcasts) mode when PAT is enabled. Applications that employ unicast for session setup (signaling) and later use multicast for data will have to be handled individually and therefore may not work through PAT.

3.2 Support for OAM ping originating from the CPE

CBOS Release 2.2.0 adds support for end-to-end pings for Operations and Administrations Maintenance (OAM) loopback cells. For example:

ping wan0-0

Initiates end-to-end loopback OAM cell

The **ping** command reports OAM Loopback success or failure, but does not report any time based or other metrics.

3.3 Support for Error log enhancements

CBOS Release 2.2.0 supports the following error log enhancements:

- All lines are marked with a timestamp designating the time elapsed since boot-up. The timestamp is the following format:

  `DDD:HH:MM:SS`

  Where DDD is the number of days, HH is hours, MM is minutes and SS is seconds.

- The error log buffer now supports 20 entries with support for entries up to 80 characters (entries over 80 characters will be truncated).

The following types of messages are supported:

- wanX up, trained rate down, trained rate up, transmit power, receive gain, receive margin, baud and line quality
- wanX down
- PPP up
- PPP down
- LCP open
- IPCP open
- IP x.x.x.x

- PPP authentication failed
- PPP TermAck ("Termination Acknowledgement")
- Specific in-band messages: Session Timeout, Session Warning, Idle Timeout, Idle Warning, Busy
- Timeout idle/session period expired
- User requested disconnect

3.4 Display for negotiated Ethernet speed

Note The following feature does not apply to the Cisco 633.

CBOS Release 2.2.0 displays the negotiated speed (10 or 100Mbps) and duplex setting of the Ethernet interface.

3.5 Support for Exec Login Null

If the Exec password is null, CBOS Release 2.2.0 refuses Telnet login and displays the message "Connection refused, password not set" or equivalent.

3.6 Support for In-band message reporting

Note The following feature does not apply to the Cisco 633. This feature also requires the Cisco 6100 Release 2.3.0.

CBOS Release 2.2.0 displays all Digital Off Hook (DOH) related in-band messages to the console.

3.7 CBOS modifications for DOH compatibility

Note The following feature does not apply to the Cisco 633.

CBOS Release 2.2.0 supports the following modifications to display DOH information:

- Default web page displays the status of ppp
- Either the exec or the enable password allows exec access
- CLI displays in-band messages

3.8 Support for a DHCP Server Duplicate Address Timer

Note The following feature does not apply to the Cisco 633.

The DHCP Server Duplicate IP address timer is now programmable, with a default of once every five seconds. This parameter is a CBOS NVRAM parameter only.

3.9 Support for a DHCP Lease Enhancement

Note The following feature does not apply to the Cisco 633.

The DHCP server now immediately removes any leased addresses from its IP address table. Previous releases removed leased addresses after 180 seconds.

3.10 Support for CHAP

Note The following feature does not apply to the Cisco 633.

CBOS Release 2.2.0 supports the Challenge Handshake Authentication Protocol (CHAP). CHAP provides more secure password authentication than the Password Authentication Protocol(PAP). Also, CHAP/PAP negotiation is auto-detected.

3.11 Support for VC Priority Queuing

CBOS Release 2.2.0 supports priority queuing of Virtual Circuits (VCs) on a per VC basis. Priority queues allows you to prioritize one VC queue over another by provisioning separate High and Low priority queues. Per VC priority queuing is an important feature in order to prioritize voice and video packets over data.

3.12 TFTP Client support

CBOS Release 2.2.0 supports the Trivial File Transfer Protocol (TFTP) client, which is a key feature needed to support the emerging configuration-less CPE architecture. CPE can now request configuration files and software loads with the TFTP client support. Previous versions of CBOS supported TFTP Server functionality only.

3.13 Support for Reboot Timer

This feature allows you to set a timer for reboot at a specified interval, which prevents you from correcting the configuration locally.

3.14 Support for Expanded Exec Level Capability

Note The following feature does not apply to the Cisco 633.

For CBOS Release 2.2.0, the Exec level password rights allow the user to:

- Bring RADSL link Up
- Bring RADSL link Down
- Set PPP userid
- Set PPP password

3.15 Support for SNMP community names

Note The following feature does not apply to the Cisco 633.

CBOS Release 2.2.0 now supports the following Simple Network Management Protocol (SNMP) community names:

- public
- proxy
- private
- regional
- core

In addition, CBOS Release 2.2.0 provides better authentication and access control by supporting a list of SNMP Managers (instead of just one). This allows the Agent (c67x) to send traps to multiple SNMP Mangers instead of one location. This allows for more secure SNMP transactions with multiple IP addresses, instead of the current one. Each manager supports a community name. Authentication failures to the Agent result in Authentication TRAP messages being sent to the list of Managers. Traps can be enabled or disabled on a per manager basis.

3.16 New Commands

The CBOS Release 2.2.0 supports the following new commands:

- **set dhcp server tick** *#seconds*

  Sets the DHCP server duplicate address checking timer.

  Note This command does not apply to the Cisco 633.

- **set ppp wan0-0 authentication** {**enabled** | **disabled**}

  Sets PAP/CHAP on or sets no PPP authentication.

  Note This command does not apply to the Cisco 633.

- **set atm pq { on | off }**

  Sets ATM prior queuing on or off.

  Note You must issue the **set atm pq** {**on** | **off** } command before issuing the **set int wan0-x priority** {**high** | **low**} command.

- **set int wan0-x priority** {**high** | **low**}

  Sets the per-VC priority.

- **tftp** {*mode*} {*host*} {*filename*}

  Allows you to download a new tftp client. The *mode* variable is either "image" or "config", *host* is the IP address of TFTP server.

- **shutdown** [**now** | **show** | **off** | <*#seconds*>]

  Enables the shutdown reboot timer.

4. Important Notes

The following section describes information important to Release 2.2.0 of CBOS.

4.1 Upgrading to CBOS 2.2.0

The upgrade process is the same whether you use the Trivial File Transport Protocol (TFTP) or serially download the new image of the CBOS software. Once the new file is written to the flash, enter the reboot command from the CBOS command line to reset your system. The new image loads, decompresses two images, and programs the new images to the correct flash memory locations.

Caution Do not reset the system or halt its operation in any way during the upgrade process. Resetting while writing a new image to flash memory ***will corrupt*** the flash.

4.1.1 TFTP Download

See the following instructions to use TFTP to download a new software image.

Step 1 Login to the Cisco equipment using the Enable password.

Step 2 Enable TFTP on the Cisco equipment.

```
set tftp enabled
```

Step 3 Determine the equipment's IP address.

```
show int eth0
```

Step 4 From the DOS window or TFTP client, TFTP the image to the CPE. In a DOS window, the command is:

```
tftp -i <ip address of CPE> put <filename>
```

Step 5 Ensure that file downloaded correctly by issuing the following command:

```
show errors
```

You should see an "Image downloaded successfully" message.

Step 6 Reboot the CPE.

4.1.2 Serial Download

To serially download the image, enter the following settings through a serial console connected to your system:

- 38.4 Kbaud
- No parity
- 8-data bits
- 1-stop bit
- No flow control

Upgrading from CBOS Version 2.1.0

See the following procedure if you are updating from CBOS Version 2.1.0:

Step 1 Issue the following command from the CBOS command line:

```
set download code
```

The CPE begins downloading.

Step 2 Initiate a serial upload with the terminal program. In Hyperterminal, this is done by selecting Transfer-->Send--> then selecting the filename to send and XModem or Xmodem1K as the protocol.

Step 3 After the upload, the CPE automatically reboots and loads the new image.

The code sequence (shown below) is an *example* of what is displayed after a new image is serially downloaded; and the system is rebooted.

```
cbos# set download code
Downloading
 -- Download complete --
    Transferred 0009e600 bytes
Hello!
Cisco Broadband Operating System self-update code: Release 2.2.0
NOTE: Do not power off the Cisco 67x until update is finished!
Decompressing router ...
Erasing FLASH ...
Programming ...
Decompressing monitor ...
Programming ...
Hello!
User Access Verification
Password:
cbos>
```

4.2 Bridging Mode Procedures

Note This section does not apply to the Cisco 633.

When the Cisco 67x operates in bridge mode, it behaves like a wire connecting a local PC directly to a service provider's network. Bridge data is encapsulated using the RFC1483 or Point-to-Point Protocol (PPP) (Bridging Control Protocol (BCP)) protocol to enable data transport. Because bridges operates at a Media Access Control (MAC) layer only, applications requiring IP communication, such as Telnet, Trivial File Transfer Protocol (TFTP), Remote Dial-In User Service (RADIUS), Syslog, Ping, and the web interface, are not available unless a management VC is configured.

Cisco currently supports a learning bridge mode. The virtual path identifier/virtual channel identifier (VPI/VCI) configuration of the Cisco 67x is unaffected by the operational mode (bridging versus routing) of the device.

Cisco also provides two methods of configuring and managing the bridged Cisco 67x, through in-band bridging management or through a separate management VC. The two methods cannot be used simultaneously. If a separate management VC is used, the Cisco 67x can only be managed remotely through WAN0-1 and not from the local network.

With rfc1483 management enabled, you can manage the router using telnet. The following commands are accessible through the managed bridge:

- **ping**
- **telnet**
- **tftp**

The following procedure shows how to set up the Cisco 67x for in-band bridging management.

Note You must be in the **enable** mode to do the procedure below. You must perform the procedure in the sequence as shown.

Step 1 To enable RFC1483 bridging, enter:
`set bridging rfc1483 enabled`

Step 2 To save your changes, enter:
`write`

Step 3 To reboot the device, enter:
`reboot`

Step 4 To enable in-band management of the bridge, enter:
`set bridging management enabled`

Step 5 To set the Ethernet interface, enter:
`set int eth0 ip <`*`ip address`*`>`

The IP address of the Ethernet port should be an IP address on the same network as that of the "far-end" station.

Step 6 To enable the Cisco 67x to direct management traffic to the far-end station, enter:
`set route default wan0-0`

Step 7 To set the default route, enter:
`set route default ip <ip address>`

The default IP address should the IP address of the far-end station that is used to telnet into the router.

Step 8 To save your changes enter:
`write`

Step 9 To enable your changes, reboot the router:
`reboot`

To manage the bridged Cisco 67x using a separate management VC, follow these steps:

Step 1 To disable in-band bridging management, enter:
`set bridging management disabled`

Step 2 To enable bridging PVC, enter:
`set bridging PVC enabled`

Step 3 To save your changes, enter:
`write`

Step 4 To reboot the device, enter:
`reboot`

After rebooting, the Cisco 67x will have two PVCs enabled. Wan0-0 is used strictly for bridged traffic, while WAN0-1 is used strictly for management traffic. Wan0-1 will be using RFC 1483 routing.

Step 5 Set an IP address on the Ethernet port that is on the same network as the far-end station out the WAN0-1 interface:
`set int eth0 ip <ip address>`

Step 6 Set the default route of the Cisco 67x to WAN0-1:
`set route default wan0-1`

For more information on using the **set bridging** command, see the *Cisco Broadband Operating System User Guide*.

The rules that govern bridging mode:

- Bridging and routing do not operate simultaneously on the Cisco 67x.
- Only one bridging mode is allowed at any one time (i.e., RFC1483 or PPP/BCP, not both). The RFC1483-support mode uses an AAL5-LLC/SNAP header. This is the default header type for most routers implementing RFC1483.
- The following commands do not work while in bridge mode:
  - **set route** (and setting static routes)
  - RIP-related commands (**set** and **show**)
  - Filter-related commands (**set** and **show**)
  - Web interface (only allowed if management is enabled)
  - RADIUS
  - Syslog

If you choose bridging as your connection mode, also see the following sections in the "Configuration Procedures" chapter of the your router's installation and operation guide:

- The "Configure the WAN Ports" section.
- The "Configure Applications" section through the "Evaluate System Activity and Performance" section.

4.3 RFC Routing Procedures

Note This section does not apply to the Cisco 633.

See the following sections for instructions on setting up your network to run the Routing Information Protocol (RIP) in RFC Routing mode.

4.3.1 Scenario #1: Assign the Cisco 67x to a subnet of the network of the terminating (Cisco 6400 or equivalent) equipment's ATM subinterface

Use the example values listed in the following table to configure the Cisco 67x accordingly:

Note The following values are examples only.

Table 3 Scenario #1--Sample Values for the Cisco 67x and the terminating equipment

Cisco 67x	Terminating Equipment
ETH0: 192.168.18.1	atm0/0/0.40
mask:255.255.255.248	ip address 192.168.18.200 255.255.255.0
WAN0-0 destination: 0.0.0.0	rip network 192.168.18.0

With the example values above, the terminating equipment accepts RIP updates when they are sent from the 192.168.18.x network coming in on the terminating equipment's ATM subinterface (atm0/0/0.40).

The benefit of this method is that you do not have to issue additional commands to the Cisco 67x.

4.3.2 Scenario #2: Assign an IP address to the WAN0-0 interface on Cisco 67x that resides on the same network as the terminating equipment's ATM subinterface

Use the example values listed in the following table to configure the Cisco 67x accordingly:

Note The following values are examples only.

Table 4 Scenario #2--Sample Values for the Cisco 67x and the terminating equipment

Cisco 67x	Terminating Equipment
ETH0: 192.168.18.100	atm0/0/0.40
netmask: 255.255.255.0	ip address 222.1.1.1 255.255.255.0
WAN0-0 destination: 222.1.1.2	rip network 222.1.1.0

If the Cisco 67x is in RFC mode and has an IP address assigned to the WAN0-0 interface, it uses that address as the source address when sending a RIP update out WAN0-0, instead of using the Ethernet interface (ETH0) address. Since the WAN0-0 destination on the Cisco 67x in this example is on the same subnet as the terminating equipment's ATM subinterface, the terminating equipment processes the RIP update it receives from the Cisco 67x.

The drawback of this scenario is that you must use an IP address on the Cisco 67x destination IP and add another configuration step. However, it is necessary due to the unnumbered nature of the Cisco 67x's DSL/ATM interface.

5. Limitations and Restrictions

The following list describes known issues and functionality details.

- When you download a new configuration file, you must name it `nscfg.xxx`, where xxx can be any extension.
- The following **enable** level commands incorrectly list on the **exec** user help screen and should be disregarded. The commands are: **show running**, **show running#**, **show nvram**, and **show nvram#**.

6. Open Caveats as of the CBOS Release 2.2.0

See the following sections for a list of open caveats for the Cisco 675/675e as of CBOS Release 2.2.0.

6.1 Open Caveats for the Cisco 633 as of Release 2.2.0

Table 5 lists open caveats for the Cisco 633 as of CBOS Release 2.2.0.

Table 5 Open Caveats for the Cisco 633 as CBOS Release 2.2.0

DDTS Entry	Description
CSCdp10731	Serial management link not active until train with certain router serial card. **Impact:** Serial data connection to 633 will not pass data until the SDSL line is trained, even on the management DLCI ser0-0. This problem occurs when connecting to routers using the PowerQUICC serial processor. The result is that the CPE can not be managed remotely via telnet on the LAN side until the SDSL line has trained. **Workarounds:** • Use the RJ-45 serial management cable to manage the CPE locally. • Connect to the 633 serial data port with a router not using a PowerQUICC processor. • Use a terminal server and local RJ-45 serial management cable if remote telnet access is necessary before the line trains.

Table 5 Open Caveats for the Cisco 633 as CBOS Release 2.2.0

DDTS Entry	Description
CSCdp11303	TFTP file put to TFTP server with port other than 69 fails. **Impact:** If the user configures the TFTP server to listen to a port other than 69 the server will not correctly use that port, but instead use port 69. **Workaround:** Use default port 69 for TFTP. This should not be a problem for most users.
CSCdp31461	Queue not maintaining bit rate. **Impact:** High priority bitrate is not maintained on the second high priority queue when multiple high priority queues are configured. **Workaround:** Only configure one VCC as being high priority if priority queuing is enabled.
CSCdp32415	Packet loss when train rates are different on same card. **Impact:** When ports 1&3 or 2&4 are trained at different rates on the same card (i.e. 1168 on port 1 and 784 on port 3) you will experience packet loss. Although the rates can be different between 1&3 and 2&4 (i.e. 1168 on ports 1&3, and 784 on ports 2&4). This will only happen when the card is trained at different rates on the same card. **Workaround:** Provision the card to have the same rates on ports 1&3 or ports 2&4. For example: Port 1: 1168 / 1168 Port 2: 784 / 784 Port 3: 1168 / 1168 Port 4: 784 / 784
CSCdp43028	Default powerscale value for version A.83 firmware is incorrect. **Workaround:** none
CSCdp43068	256k rate shows up as 272k. **Impact**: The 633/673 cannot be set for a rate of 256k. **Workaround:** Set the rate of the 633/673 to be 272k.

6.2 Open Caveats for the Cisco 673 as of Release 2.2.0

Table 6 lists open caveats for the Cisco 673 as of CBOS Release 2.2.0.

Table 6 Open Caveats for the Cisco 673 as CBOS Release 2.2.0

DDTS Entry	Description
CSCdp16512	User unable to add interface name as a gateway via web interface **Impact:** User tries to add interface, such as the wan0-0, as a gateway via the web interface. **Workaround:** Configure the interface as a gateway using the CLI
CSCdp17068	TFTP on alternate port not functioning. **Impact:** The TFTP application will not function on alternate application ports. **Workaround:** use the default port (69) for TFTP purposes.
CSCdp18490	DEBUG BERT command does not work. **Impact:** User enters "debug bert" at enable level via CLI and it does not work. **Workaround:** BERT is not implemented in 673. Don't use the debug **bert** command.

Table 6 Open Caveats for the Cisco 673 as CBOS Release 2.2.0

DDTS Entry	Description
CSCdp23073	Using DHCP client with NAT and DHCP server gives incorrect results. **Imapct:** User gets wrong address pool since the DHCP server giving the CPE an IP address pool does not how NAT is setup. **Workaround:** Do not use the DHCP client with NAT and DHCP server.
CSCdp23086	DHCP client not working over wan0-0. **Impact:** The DHCP client feature does not take the DHCP address/mask offered to it by the server and use it as eth0 address/mask of CPE, when the server is out the wan0-0 port. **Workarounds:** • Use a DHCP server that exists on the ethernet link of the 673. • Use RADIUS for dynamic address assignment. • Use IPCP pools for dynamic address assignment.
CSCdp24230	Syslog not reporting link state or ppp open states. **Impact:** The syslog application does not report all pertinent data. (WAN port train, link quality, speed). **Workaround:** Use the "set error module xxxxx" combined with: "set error debug enable". With "xxxxx" = the type of error reporting you would like to be sent to the syslog server. Some error modules, such as link quality and speed, will still not be reported correctly to a syslog server.
CSCdp31758	Bridging management should be disabled/not allowed in other modes. **Impact:** Bridge management option available when not in bridging mode. Could cause connection/routing problems when enabled in routing mode. **Workaround:** Do not enable bridge management when CPE is in PPP or RFC routing mode.

6.3 Open Caveats for the Cisco 675/675e as of Release 2.2.0

Table 7 lists open caveats for the Cisco 675/675e as of CBOS Release 2.2.0.

Table 7 Open Caveats for the Cisco 675/675e as CBOS Release 2.2.0

DDTS Entry	Description
CSCdm08268	stats ip WAN0-0 does not display correct packet statistics. **Impact:** Command "stats ip WAN0-0" always displays 0 stats. **Workaround:** None.
CSCdm11515	NVRAM is not written when configuration is made on the Web. **Impact:** Changes made on the web are only good until the cpe is rebooted. **Workaround:** Use CLI interface to make permanent changes.
CSCdm36544	2.4:Web filter reports WAN0-1 as all interfaces **Impact:** Web interface displays incorrectly. **Workaround:** None.
CSCdm49278	OAM F5 Segment Cell sent as F5 End-to-End Cell **Impact:** ping WAN0-x -s sends OAM F5 End-to-End cell instead of OAM F5 Segment cell. **Workaround:** None at this time.

Table 7 Open Caveats for the Cisco 675/675e as CBOS Release 2.2.0

DDTS Entry	Description
CSCdm50936	Telnet to c675 from Sun WS adds extra characters at password prompt. **Impact:** Garbage characters are displayed at password prompt. **Workaround:** User must backspace over garbage characters to enter password.
CSCdm55247	ATM OAM Pings do not appear to reflect end-to-end versus segment. **Impact:** Pings may increment the wrong set of statistics and send out the wrong type of ping (end-to-end loopback versus segment.). **Workaround:** None
CSCdm55340	IP Filters for deny all will take precedence over any other allow **Impact:** Filters functionality is currently not working. **Workaround:** None
CSCdm68034	Change start address for DHCP pool **Impact**: DHCP gateway is first address in DHCP pool **Workaround:** None. Feature request to be addressed next release.
CSCdm72771	Must write and reboot for snmp changes to take effect. **Impact:** when configuring the 675 to properly respond to snmp queries, you must specify the remote snmp manager information such as ip address and read/write capability. These configuration changes don't take affect until write and reboot of 675. **Workaround:** Must write and reboot 675 for config changes to take place.
CSCdm73505	Static routes not in routing table if gateway is ETH0 and ipcp address. **Impact:** if you add a static route to a network on the ethernet side of a 675, you must specify the ETH0 address as the gateway. However, if the ETH0 address is obtained strictly via IPCP, the static route will not appear in the routing table. **Workarounds:** • Manually assign the ETH0 address to the same ip as assigned by IPCP. This is less than ideal if the IPCP-ed address changes after every train by the 675. • Assign an address to a VIP interface on 675, and set up static route to use that address as the gateway. This is an easier workaround but may burn an ip address.

7. Resolved Caveats as of the CBOS Release 2.2.0

The following tables list all resolved caveats as of the CBOS Release 2.2.0.

7.1 Resolved Caveats for the Cisco 633

Table 8 lists all resolved caveats for the Cisco 633 as of the CBOS Release 2.2.0.

Table 8 Resolved Caveats for the Cisco 633 as of Release 2.2.0

DDTS Entry	Description
CSCdm54022	633 - no stat commands for ser0, ser0-0 .. ser0-4.
CSCdm54028	633 - can not configure dlcis on ser interfaces.
CSCdm54031	633 - need pin status on frame relay serial connector.
CSCdm54036	633 - show int does not list all interfaces.

Table 8 Resolved Caveats for the Cisco 633 as of Release 2.2.0

DDTS Entry	Description
CSCdm54037	633 - uptime always show 0 time up.
CSCdm54038	633 - help command not correct for int ser0-x.
CSCdm54039	633 - addressing ser0-1 gives cryptic error message.
CSCdm55957	633 - set int wan0 mode shows up twice in config.
CSCdp10092	Shutdown command not present at exec or enable menus.
CSCdp10101	TFTP command produces garbage when typed at exec prompt.
CSCdp10108	Help text for Set error module command has typo.
CSCdp10112	**Set errors module fr** command does not have confirmation message.
CSCdp10118	**Set errors module none** command displays bad confirmation message.
CSCdp10125	**Set errors module telnet** command displays no confirmation message.
CSCdp10128	**Set** command appears in the exec mode menu.
CSCdp10720	Routing table does not update until write/reboot.
CSCdp10744	Must write and reboot after changing DLCI.
CSCdp10720	Routing table does not update until write/reboot.
CSCdp10754	**show rfc** only shows first two wan PVCs.
CSCdp10756	User can enter **set int ser0-0 enable/disable**. Command not in help.
CSCdp11313	Changing of telnet port/remote IP needs write/reboot message.
CSCdp11520	**set int wan0** down does not survive reboot.
CSCdp11524	**set int wan0** scrambling en/dis in CBOS but not functioning.
CSCdp11861	**set SNMP traps** and enabled fail to reboot.
CSCdp15509	**shutdown X** command not functioning properly.
CSCdp15547	Autoupdate program shows 67x product title.

7.2 Resolved Caveats for the Cisco 673

Table 9 lists all resolved caveats for the Cisco 673 as of the CBOS Release 2.2.0.

Table 9 Resolved Caveats for the Cisco 673 as of Release 2.2.0

DDTS Entry	Description
CSCdp16864	Filter button in web interface missing, but still active.
CSCdp16502	Web interface reports 673 as 675 in intro text.
CSCdp17017	Syslog not functioning without performing a debug syslog.
CSCdp17098	Error log does not show WAN port messages.
CSCdp17132	Not able to add routes with reachable gateways.
CSCdp17177	Cannot set wan link up/down from exec prompt per PRD.
CSCdp18497	User can defined DHCP pools of less than zero.
CSCdp21410	**write** fails after serial download of config.
CSCdp21962	Debug menu has entries not valid for product.

Table 9 Resolved Caveats for the Cisco 673 as of Release 2.2.0

DDTS Entry	Description
CSCdp28269	c673 does not initiate train upon reboot; crashes w/set int wan0 up.
CSCdp28282	673 self-update screen shows c633 product name.
CSCdp28353	All logical wan ports have vpi/vci=0/0 and cannot be changed.
CSCdp29713	On-line help for set download command not working w/ '?' command.
CSCdp31744	Can not set VCI=4 on logical wan port.
CSCdp31755	Can assign same IP address to different VIP interfaces.

7.3 Resolved Caveats for the Cisco 675/675e

Table 10 lists all resolved caveats for the Cisco 675/675e as of the CBOS Release 2.2.0.

Table 10 Resolved Caveats for the Cisco 675/675e as of Release 2.2.0

Bug Number	Description
CSCdk87915	OAM loopback is not functioning correctly.
CSCdm28690	DHCP pool size one less with IPCP learn enabled.
CSCdm29153	c675: certain password characters cause nvram viewing probs.
CSCdm58895	C675: DHCP Server Unable to NAK Address Request from MS Win Client.
CSCdm39578	subnetmask negotiated via IPCP incorrectly applied to ETH0.
CSCdm55251	DHCP error messages scroll forever.
CSCdm61177	Output for the show route is incorrect.
CSCdm63511	Changing Application Ports should have write/reboot message.
CSCdm65723	Deleted routes not removed from running configuration.
CSCdm65731	When WAN0-0 is terminated multiple vcs not displayed.
CSCdm65739	set int WAN0-0 close will allow port to re-open.
CSCdm67107	DHCP Relay does not forward packets over wan interfaces.
CSCdm67117	set dhcp client on does not turn off dhcp relay agent.
CSCdm67120	DHCP Client does not work completely with Windows NT DHCP Server.
CSCdm67276	web: WAN0-0 uname & pword limited to 8 characters.
CSCdm67716	PC unable to get WINS server address from 675 DHCP server.
CSCdm68028	DHCP poolsize is incorrect.
CSCdm69663	NAT - setting outside IP manually does not work after reboot.
CSCdm71347	Static route entry to network has wrong netmask.
CSCdm71362	Manual deletions from NVRAM leave carriage return in config.
CSCdm73505	static routes not in routing table if gw is ETH0 and ipcp address.
CSCdm79029	Session/Idle Timers not passed to 675 from 6100 rev 2.25.

8. Information from Previous Releases

The following new features are supported by CBOS Release 2.1.0. Each feature is described in the subsections indicated in parentheses.

- Supports Ethernet and ADSL Interface elements for the Enterprise MIB
- Supports RFC1483 Routing
- Provides primary and secondary WINS and DNS support for IPCP and DHCP server
- Provides an IPCP subnet mask option for PPP and DHCP server
- Supports enabling and disabling of DOH Mode
- Supports automatic enabling and disabling of PAP
- Supports a DHCP Relay Agent (plus Enterprise MIB Support)
- Supports virtual IP addresses
- Support for enhancements to DHCP Server
- Support for enhancements to NAT
- Support for multicast proxy option
- Support for clearing the ARP Table, IPCP Parameters, and passwords
- Support for the filtering of broadcast and multicast packets

9. Related Documentation

Use these release notes in conjunction with the documents listed in this section.

- *Cisco Broadband Operating System User's Guide*
- *Cisco 633 SDSL Modem Installation and Operation Guide*
- *Cisco 673 ADSL Router Installation and Operation Guide*
- *Cisco 675 ADSL Router Installation and Operation Guide*
- *Cisco 675E ADSL Router Installation and Operation Guide*

10. Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note Support for this product is normally provided by your service provider. Please contact your service provider for your first level of support. If you need technical assistance and have purchased this product directly from Cisco or have a support contract with Cisco, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com."

---

11. Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

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

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