

Cisco Broadband Operating System 2.3.0 Release Notes

Dec 21, 2000

These release notes describe new features, important caveats, resolved issues, and the software upgrade process for the Cisco Broadband Operating System (CBOS) Release 2.3.0. 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 21. Information about electronic documentation can be found in the “Obtaining Documentation” section on page 21.

Contents

These release notes provide the following information:

- Cisco Broadband Operating System, page 2
- New Features for CBOS Release 2.3.0, page 2
- Upgrading to CBOS Release 2.3.0, page 12
- RFC 1483 Routing, page 15
- Resolved Issues in CBOS Release 2.3.0, page 16
- Known Issues in CBOS Release 2.3., page 0 17
- Information from Previous Releases, page 20
- Related Documentation, page 21
- Obtaining Documentation, page 21
- Obtaining Technical Assistance, page 22



Cisco Broadband Operating System

CBOS is the common operating system for Cisco customer premises equipment (CPE). The CBOS is modeled after Cisco IOS software 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 2.3.0 supports the following Cisco CPE products:

- Cisco 627
- Cisco 633
- Cisco 673
- Cisco 675
- Cisco 675e
- Cisco 677
- Cisco 678

New Features for CBOS Release 2.3.0

Port Address Translation Enhancements

CBOS Release 2.3.0 adds Port Address Translation (PAT) enhancements as discussed in the following sections.

Support for Microsoft WINS Applications

CBOS Release 2.3.0 adds PAT support for Microsoft WINS-based applications:

- Microsoft's Network File Sharing
- Browsers to view Microsoft's Network Neighborhood

Support for UDP Broadcast

CBOS Release 2.3.0 adds PAT support for UDP network-directed as well as subnetwork-directed broadcasts.

Support for Remote Shell (rsh), Remote Copy (rcp), and Remote Login (rlogin)

CBOS Release 2.3.0 adds PAT support for non-encrypted remote shell (rsh), remote copy (rcp), and remote login (rlogin) protocols.

Network Address Translation Enhancements

CBOS Release 2.3.0 adds Network Address Translation (NAT) enhancements that allow NAT to be applied to each interface. This means you can apply NAT to the Ethernet, logical WAN interfaces and the VIPs (virtual interfaces). With the latest NAT enhancements, eth0, vip0 through vip2 can be configured as inside or outside interfaces and wan0-0 through wan 0-3 can be configured as outside interfaces for NAT.

When NAT is enabled, NAT translates only inside to outside and outside to inside traffic. Traffic that remains within its own respective boundary (inside to inside or outside to outside) is not translated.

NAT Commands with No Changes

Use the current commands to globally configure interface timeout values. No new commands are added to create dynamic NAT table entries because the network generates these based on traffic. The NAT commands in Table 1 have not changed:

Table 1 NAT Commands with No Changes

Command	Description
set nat { enable disable }	Global on and off command for all interfaces
set nat disable	Disables NAT on all interfaces
set nat entry add	Adds a static NAT entry
set nat entry delete	Deletes a static NAT entry
set nat outside ip address	Adds a specific static NAT entry to the WAN0-0 table
show nat	Displays all NAT entries, including static and wildcard Wildcard entries display as asterisks.

NAT Commands with Changes

Table 2 lists new commands to set NAT protocols for specific interfaces.

Table 2 NAT Commands with Changes

Command	Description
set nat outside ip ip address	Sets Outside Global IP Address for the WAN0-0 Interface as in CBOS 2.2
set interface wan0-1 outside ip 172.167.20.42	Sets a specific outside IP address for WAN0-1 interface
set int eth0 inside	Sets ETH0 interface as an inside network
set int vip0 inside	Sets virtual interface 0 as an inside network



Note

The command **set interface eth0 outside ip address** is invalid.

Enhancements to the **show nat** command includes the NAT Status and Network Side for all Interfaces. The following is an example of the new format:

sh nat Example

```
cbos#sh nat
```

```
NAT is currently enabled
```

Port	Network	Global
eth0	Inside	
wan0-0	Outside	192.161.23.4
vip0	Outside	
vip1	Outside	
vip2	Outside	

Local IP	Port	Global IP	Port	Timer	Flags	Proto	Interface
*****		*****		0	0x3041	***	eth0

Support for IP Precedence

CBOS Release 2.3.0 recognizes IP Precedence bits defining Type of Service (TOS) in the IP header and routes IP packets based on this value. With this enhancement, you can use IP Precedence to route packets to a specific interface.

IP Precedence bits map to individual interfaces according to the following rules:

- One or more IP precedence values can be mapped to one interface.
- A particular IP Precedence value can be mapped to only one interface for the same destination IP address range.
- The gateway specified for the route must be the same as the interface transmitting the packet.

IP Precedence bits route IP packets to individual interfaces according to the following rules:

- If an IP packet specifies an IP Precedence value mapped to an interface, the interface forwards the IP packet
- If an IP packet has an IP Precedence whose value does not map to a specific interface, the packet is forwarded normally.
- If an IP packet has a matching precedence but not matching destination, the packet is forwarded using the default precedence route, if configured

New extensions to the CBOS Release 2.3.0 CLI allow users with enable-level access to configure and map IP Precedence values to different interfaces. The syntax for the new command is:

```
set route add ip ip_address gateway gw_address precedence n
```

Table 3 shows examples of this command.

Table 3 Sample IP Precedence Setting Commands

Command	Description
set route add ip 192.200.1.0 gw 192.100.10.1 precedence 5	Routes packet from network 192.200.1.0 with a precedence of 5 to the gateway at 192.100.10.1
set route add ip 192.200.1.0 gw wan0-1 precedence 5	Sets IP Precedence to 5 for gateway interface
set route default wan0-1 precedence 5	Sets a default route for precedence 5 packets to wan0-1

The **set route** command can accept either an IP address or an interface as valid entries according to the command syntax **set route default { ip-address | interface }** or **set route add ip ip-address gw { ip-address | interface }**. When using IP address as a gateway, the gateway address must exist in one of WAN interfaces. Use **show route** to display WAN addresses.

Enhancements to the **set route default** command include a precedence field that defines the default routes for packets with Precedence bits set. The syntax for the set route default command is:

set route default { ip address | interface } precedence n

The **show route** command now includes a column [P] showing the precedence level. The following is an example of the new format:

```
#show route
[TARGET]           [MASK]           [GATEWAY]        [M] [P] [TYPE]      [IF]      [AGE]
0.0.0.0            0.0.0.0          0.0.0.0          1   SA   WAN0-0      0
0.0.0.0            0.0.0.0          0.0.0.0          1   5 SAR  WAN0-1      0
192.168.10.0       255.255.255.0    0.0.0.0          1   LA   ETH0        0
192.168.1.0        255.255.255.0    0.0.0.0          1   A    WAN0-0      0
192.168.2.0        255.255.255.0    0.0.0.0          1   AR   WAN0-1      0
WAN Interfaces...
192.168.1.72       255.255.255.255  0.0.0.0          1   HA   WAN0-0      0
192.168.2.72       255.255.255.255  0.0.0.0          1   HA   WAN0-1      0
192.168.3.72       255.255.255.255  0.0.0.0          1   HA   WAN0-2      0
```

Support for TFTP Checksum

CBOS Release 2.3.0 enhances its TFTP Client and Server programs to perform checksum validation for image and configuration file transfers. Image and configuration files will be written to NVRAM only after a successful checksum validation.



Caution

The running configuration will be deleted when a TFTP file transfer is done.

New Default Settings

CBOS Release 2.3.0 defines new factory default settings. These settings apply to the Cisco 675 only:

```
set ppp wan0-0 ipcp 0.0.0.0
```

```
set ppp wan0-0 dns 0.0.0.0
```

```
set ppp wan0-0 subnet 0.0.0.0
```

```
set multicast forwarding disabled
```

```
set broadcast forwarding disabled
```



Note

The **show run** command does not show these services as enabled. Default settings are not displayed in the running configuration.

Support for GSI 3.2 Firmware Update

The GSI 3.2 firmware update provides for lower baud rates to the 17 Kbaud and 64 Kbaud. CBOS Release 2.3.0 supports these rates in the Cisco 675 and 675e. The Cisco 677 can support these rates after downloading the CBOS Release 2.3 image. Service providers now have wider range of desirable rates from which to choose for these products. (See Table 4 and Table 5.)

Table 4 Downstream Channel Bit Rate per Constellation Size (kb/s)

Symbol Rate (Kbaud)	Signal	Bit Rate per Constellation Size (kb/s)						
		256 uncoded	256	128	64	32	16	8
136	Payload with RS	1024	896	768	640	512	384	256
340	Payload with RS	2560	2240	1920	1600	1280	960	640
680	Payload with RS	5120	4480	F/A	3200	F/A	1920	F/A
952	Payload with RS	7168	6272	F/A	4480	F/A	2688	F/A

RS = Reed-Solomon error correction

F/A = Future Availability

Table 5 Available Downstream/Upstream Baud Rates

Downstream Kbaud	Upstream Kbaud
136	17
136	68
136	136
340	68
340	136
680	136
952	136

The **show rates** command now includes entries with the additional baud rate combinations. The following is an example of the additional listings:

```

cbo#show rates
Possible ATM/ADSL Line Rates
Downstream                Upstream (Kbps)
-----
952 Kbaud Downstream ----- 136 Kbaud Upstream
7168                      1088
6272                      952
4480                      680
2688                      408
-----
680 Kbaud Downstream ----- 136 Kbaud Upstream
5120                      1088
4480                      952
3200                      680
1920                      408
-----
340 Kbaud Downstream ----- 136 Kbaud Upstream
2560                      1088
2240                      952
1920                      816
1600                      680
1280                      544
960                       408
640                       272
                          91
340 Kbaud Downstream ----- 68 Kbaud Upstream
2560                      544
2240                      476
1920                      408
1600                      340
1280                      272
960                       204
640                       136
                          45

```

```

-----
136 Kbaud Downstream ----- 136Kbaud Upstream
1024                               1088
896                               952
768                               816
640                               680
512                               544
384                               408
256                               272
136 Kbaud Downstream ----- 68 Kbaud Upstream
1024                               544
896                               476
768                               408
640                               340
512                               272
384                               204
256                               136
                               45
136 Kbaud Downstream ----- 17 Kbaud Upstream
1024                               136
896                               119
768                               102
640                               85
512                               68
384                               51
256                               34
                               11

```

CBOS Modifications for Setting Upstream Transmit Power

New extensions to the CBOS Release 2.3.0 CLI allow a user with exec-level access to set the upstream transmit power. The syntax for the command is:

```
set interface wan0 txpower value_in_db
```

Valid values are:

- 1 = full
- 2 = -3 db
- 3 = -6 db
- 4 = -9 db
- 5 = -12 db
- 6 = -15 db

Enhancements to DHCP Pool Start Addressing

CBOS Release 2.3.0 enables you to learn the starting addresses for the DHCP pool. CBOS Release 2.3.0 enhancements use the mask learned during IPCP negotiation to define the range of IP addresses.

Enhancements to WAN-LNK LED Blink Pattern

CBOS Release 2.3.0 adds new blink patterns to the WAN Link LED to indicate the connection state of the Cisco 675 in more detail.

Blink Pattern/Rate	Description
Steady ON	A link is established to the WAN port. All parameters for physical and logical connections are correctly set. The equipment successfully transmits and receives data.
Continuous rapid blinking, about 3 blinks per second	The equipment is trying to establish a connection. The pattern continues until a connection is established.
Intermittent blinking. For the Cisco 675: 6 rapid blinks followed by a 2-second pause before repeating. For the Cisco 676 or 677: 5 rapid blinks followed by a 2-second pause before repeating.	The equipment is trying to establish a physical connection. At this time, the training session is not yet completed; there are no logical connections and negotiated line conditions with other equipment (such as DSLAMs) are not yet established.
OFF	Check all connections. Ensure the WAN0 interface is not disabled.

Enhancements to the Set Filter Command

Use the **set filter** command to specify and modify IP filtering conventions for the Cisco 67x.

```
set filter {code} {on | off | reset} [deny | allow] {incoming | outgoing} {interface eth0 | wan0-0  
| all} {src-ip src-mask dest-ip dest-mask} [protocol TCP | UDP | ICMP] [srcport lo - hi]  
[destport lo - hi]
```

Syntax Description

<i>code</i>	Enter the filter number to be modified. Valid filter code values are 0 through 19.
on off reset	Enables, disables or resets the filter. Reset allows you to reset a filter to default values without removing an entire configuration.
deny allow	Specifies whether the filter is to allow or deny packets that match the filter's address and mask.
incoming outgoing	Specifies direction of traffic to be filtered; required.
<i>interface</i> eth0 wan0-0 all	Displays the Interface on which to apply the filter. This can be a particular interface such as eth0 or wan0-x or all interfaces.
<i>src-ip</i>	Enter the source IP address for packets.
<i>src-mask</i>	Enter the mask to be applied to source IP address. This allows the filter to match a group of incoming IP addresses.
<i>dest-ip</i>	Enter the destination IP address of outgoing packets.
<i>dest-mask</i>	Enter the mask to be applied to destination IP address. This allows the filter to match a group of outgoing IP addresses.
protocol TCP UDP ICMP	Specify which protocol to match; optional.

srcport <i>lo - hi</i>	Displays the inclusive range of source port numbers to block; 1 - 65535 matches all source ports.
destport <i>lo - hi</i>	Displays the inclusive range of destination port numbers to block; 1 - 65535 matches all destination ports.

Command Mode

Enable

Usage Guidelines

Use the **set filter** command to specify IP filtering conventions. The Cisco 67x has 20 filters that can be applied to TCP, UDP and ICMP packets passing through the router's interfaces. Enabled filters are applied to packets in sequential order according to filter number.

The rules that govern the **filter** command are:

- The minimum parameters required for the **set filter** command are the filter code and the on/off/reset flag.
- A parameter can be implemented only if all previous parameters are implemented, even with don't care values. If you want to use the protocol parameter, all required and optional parameters prior to the protocol parameter must be included.
- If no filters are enabled, no filters are checked. If at least one filter is enabled, the filter function proceeds through the list of filters until a match is found. The function then returns the value of the deny | allow parameter. If no match is found, the function denies the packet.
- For traffic you want to allow, be sure that filters are enabled for allowing packets in both directions.
- Place filters for expected heavy traffic early in the list of filters. Placing frequently matched filters higher in the list maintains routing performance.
- The first match determines the fate of the packet. There are no exceptions to this rule.
- Source and destination IP address and masks must both be present on the command line when the **deny | allow** flag is present.
- A *source-address and source-mask* of 0.0.0.0 and 0.0.0.0 are used to always match a packet for the filter. Likewise, an address/mask of 255.255.255.255/255.255.255.255 is used to never match a packet.
- Filters are applied to the Ethernet interface (eth0) by default. Include the *interface variable* on the command line to specify another interface, or **all** to specify all interfaces in the router.
- Changes made to the filters will become effective immediately. Packet filtering can be globally suspended and resumed with the **set filter** command.
- All filter related commands (**set** and **show**) are disabled when in bridge mode.

Examples

The following example blocks all web access.

```
set filter 0 on deny all 0.0.0.0. 0.0.0.0 0.0.0.0. port 80
```

The following example blocks all telnet access from the 192.168.0.25 network.

```
set filter 1 on deny all 192.168.0.0 255.255.255.0 0.0.0.0 0.0.0.0 port 23
```

The following example accepts telnet access from the host 192.168.0.25.

```
set filter 2 on allow all 192.168.0.25 255.255.255.255 0.0.0.0 0.0.0.0 port 23
```

The following example blocks all FTP access on a wan port.

```
set filter 3 on deny wan0-1 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 port 21
```

The following example turns off the first filter.

```
set filter 0 off
```



Note

Press enter only after entering all command parameters. A command may appear on two lines here for readability.

Upgrading to CBOS Release 2.3.0

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

Two files make up the CBOS Release 2.3.0. One file contains an image for upgrading systems with CBOS 2.2 release software. The second file contains the an image with CRC headers and platform identifiers. These headers and identifiers validate image and configuration file transfers for supported platforms. This second file is for upgrading systems with CBOS 2.3 or subsequent releases.

Upgrading from CBOS 2.2

Download the file named **nsrouter.c6xx.2.3.0.053.bin** where c6xx is your platform. For example, c675. This file cannot be validated by the TFTP checksum feature. Use a terminal emulation application such as Hyperterminal to download the image.

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



Note

Serial downloads at this setting take approximately 5 minutes to complete.



Caution

Downloading the image with the CRC headers onto a CBOS 2.2 system will result in a *No router image present* error when the CPE is rebooted. To recover, use the monitor's xmodem download procedure:

```
es 0
es 1
es 2
es 3
es 4
es 5
df 10008000
fee00000 <byte size reported by df command>
```

If you are upgrading on a Cisco 62x, the last line should be:

```
pb 10008000 fef00000 <byte size reported by df command>
```



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 memory. The router will not reboot. Use the monitor's xmodem download procedure to recover.

Sample output

The following shows a sample output of a successful image download:

```
Ron960 User Interface:Build 111 (Jan 30 2000 17:25:27)
NetSpeed HomeRunner(TM); i960 JX; JA step number 03
Copyright 1997 NetSpeed Corporation
Copyright 1998, 1999 Cisco Systems
=>es 0
Erasing sector 00000000...
Sector erased
=>es 1
Erasing sector 00000001...
Sector erased
=>es 2
Erasing sector 00000002...
Sector erased
=>es 3
Erasing sector 00000003...
Sector erased
=>es 4
Erasing sector 00000003...
Sector erased
=>es 5
Erasing sector 00000003...
Sector erased
=>df 10008000
Downloading
CCCCCCCCCC
-- Download complete --
   Transferred 000ce000 bytes
=>pb 10008000 fee00000 ce000
Programming flash address 00000000 from 10008000...
Flash programmed
=>rb

Hello!
C67x self-update code:Release 2.3.0
NOTE:Do not power off router until update is finished!


Decompressing router...
Erasing FLASH.....
Programming...
Decompressing monitor...
Erasing FLASH.....
Programming...
Finished. Rebooting...
Hello!
Expanding CBOS image...
CBOS v2.3.0.053 - Release Software
```

Upgrading from CBOS 2.3 or later

Download the file named **c6xx.2.3.0.053.bin** where c6xx is your platform. For example, c675. This file is validated by the TFTP checksum feature. Use TFTP to download the image.

TFTP Download

Follow these instructions to use TFTP to download a new software image:

-
- Step 1** Log in 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, use TFTP to send the image to the CPE. In a DOS window, the command is:
tftp -i <ip address of CPE> put <filename>
-  **Note** Download the file named **c6xx.2.3.0.053.bin** where c6xx is your platform.
- Step 5** Ensure that the file downloaded correctly:
show errors
You should see an "Image downloaded successfully" message.
- Step 6** Reboot the CPE.

RFC 1483 Routing

This section provides two scenarios with instructions for setting up your network to run the Routing Information Protocol (RIP) in RFC Routing mode.

Scenario 1— Assign the Cisco 675 to a subnet of the network of the terminating (Cisco 6400 or equivalent) equipment's ATM subinterface

Table 6 provides sample values to configure the Cisco 675 for Scenario 1:



Note The values in Table 6 are examples only.

Table 6 Scenario 1—Sample Values for the Cisco 675 and the Terminating Equipment

Cisco 675	Terminating Equipment
ETH0: 192.168.18.1	atm0/0/0.40
mask:255.255.255.0	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 enter additional commands to the Cisco 675.

Scenario 2—Assign an IP address to the WAN0-0 interface on Cisco 675 that resides on the same network as the terminating equipment's ATM subinterface

Table 7 provides sample values to configure the Cisco 675 for Scenario 2:



Note

The values in Table 7 are examples only.

Table 7 Scenario 2—Sample Values for the Cisco 675 and the Terminating Equipment

Cisco 675	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 675 is in RFC 1483 Routing Mode with 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. The Cisco 675 does this because the WAN0-0 destination on the Cisco 675 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 675.

The drawback of this scenario is that you must use an IP address on the Cisco 675 destination IP and add another configuration step. However, it is necessary due to the unnumbered nature of the Cisco 675's DSL/ATM interface.

Resolved Issues in CBOS Release 2.3.0

Table 8 lists resolved issues for CBOS 2.3.0 and the affected platform.

Table 8 Resolved Issues for CBOS Release 2.3.0

ID Number	Description	Platform
CSCdm68034	Change start address for DHCP pool	c675
CSCdm74503	Idle/Session Timers do not appear in Commander	c675
CSCdm72771	Must write and reboot for snmp changes to take effect	c675
CSCdm81528	NAT 675/677 Session hangs when FTPing from outside to inside	c675
CSCdm81555	Timers set in CPE not working properly with Commander	c675
CSCdm82119	Timeouts keep counting after link drops; only reset when ppp opens	c675
CSCdm84893	Should be a command on the 633 to set the Serial port clock rate	c633
CSCdp19119	BNCP confreq (PPP-bridging) rejected by CPE	c677
CSCdp23035	When 633 is DCE it need clock setting capability	c633
CSCdp23263	Getting the interface data via snmp causes the cpe to hang	c675

Table 8 Resolved Issues for CBOS Release 2.3.0

ID Number	Description	Platform
CSCdp23376	The CLI virtual circuit close command closes all VCs	c675
CSCdp20428	The snmp agent is not returning the correct data to the client	c675
CSCdp27928	cbos: Dynamic NAT entry must be purged when CPE re-trains	c675
CSCdp28271	cbos:Bridging over PPP does not work	c675
CSCdp31628	cbos: TFTP Server Busy Message Is Desirable	c675
CSCdp53704	Session and/or idle time-out is broken for RFC1483 routing	c675
CSCdp56213	cbos:snmp poll will crash cpe	c675
CSCdp57385	cbos:change eth0 addr. should not require wan0 retrain	c675
CScdp57644	cbos:SNMP trap doesn't work across wan link	c675
CSCdp59188	cbos:Inside Global overwritten by Eth0 IP if changed while CPE up	c675
CSCdp59195	idle time-out is broken for RFC1483 Bridging	c675
CSCdp62828	cbos:Upstream traffic stops after few hours on the 633	c633
CSCdp63343	DSL dhcp lease resets at 1000	c677
CSCdp63351	cbos: R1483 routing rip sources the wrong address	c675
CSCdp65240	cbos: snmp manager shows cpe 677 eth int. table mtu value 4096	c677
CSCdp71438	cbos: DHCP server logic broken under RFC1483 routing	c675
CSCdp77582	Cannot add static route a c675	c675
CSCdp84257	DHCP server leased timer does not reset.	c675
CSCdp84289	SNMP: the community string should be case sensitive	c675
CSCdp86174	cbos: SNMP trap always use public instead of the configured community name	c675

Known Issues in CBOS Release 2.3.0

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 do not appear on the **exec** user help screen: **show running**, **show running#**, **show nvram**, and **show nvram#**.

Table 9 lists known issues, conditions, and workarounds for CBOS Release 2.3.0.

Table 9 *Open Issues for CBOS Release 2.3.0*

ID Number	Description
CSCdp67794	<p>cbos: SNMP variable changes should be written in NVRAM or run cfg</p> <p>Description : CPE SNMP SET variables are not retrained in the NVRAM when they are changed using the SNMP manager.</p> <p>Condition : SNMP variables state are reverted back to the previous "NVRAM" write. This affects the 67x CPEs.</p> <p>Workaround: Use the CLI method to configure the CPE.</p>
CSCdp63489	<p>cbos: Data-traffic halts if in-band management via telnet is access</p> <p>Description : Accessing the CPE using the in-band management interface ATM0 of the 627 CPE will halt traffic on other VCs. This problem only appears for the in-band access on ATM0. ATM0 is the subscriber-side interface.</p> <p>Condition : Connectivity for the other VCs is lost. This affects the 627 CPE.</p> <p>Workaround: There is no workaround. Use the console port for management.</p>
CSCdp55551	<p>cbos:Downstream performance with 512 byte packets stops after few hours</p> <p>Description : Uni-direction downstream traffic stops after the 677 CPE is subjected to the maximum theoretical throughput of 8032 KBPS trained rate. This occurs after few hours.</p> <p>Condition : Traffic stops after few hours. This affects the 677 CPE.</p> <p>Workaround: There is no workaround. The CPE needs to be rebooted.</p>
CSCdp36895	<p>cbos: priority queuing is not working properly</p> <p>Description : Traffic prioritization policy is not maintained when the aggregate traffic flow exceeds the maximum upstream trained rate.</p> <p>Condition : High priority traffic may be lost due to traffic contention. This affects the 67x and 633 CPE.</p> <p>Workaround: There is no workaround.</p>
CSCdm55247	<p>ATM OAM Pings dont appear to reflect end-to-end vs segment</p> <p>Description : ATM Segment OAM ping don't work.</p> <p>Condition : Segment OAM is treated as End-to-End OAM ping when issued from the CLI. This affects the 67x CPE.</p> <p>Workaround: There is no workaround.</p>
CSCdp88574	<p>cbos: WINS registration with inside IP address if wildcard entry is cfged</p> <p>Description : Under a NATed enviroment, the private address (WINS Client) are registered to the outside WINS-Servers (public addresses) if a static wildcard NAT entry matching the inside IP address of the WINS Client is configured on the CPE.</p> <p>Condition : Private IP addresses are returned in the WINS name resolution. This affects the 67x CPEs.</p> <p>Workaround: Don't configure a wildcard NAT entry (ie :set nat entry add 10.0.0.2) instead use a NAT entry which contains the protocol type. (ie: set nat entry 10.0.0.2 137 udp)</p>

Table 9 Open Issues for CBOS Release 2.3.0

ID Number	Description
CSCdp81895	<p>cbos: CBOS infrequently faults when eth0 ip changed from telnet session</p> <p>Description : Changing the ethernet ip address of the CPE from a telnet session may cause the CPE to exit abnormally. This occurs infrequently.</p> <p>Condition : Connectivity/access to the CPE is lost. This affects the 67x CPEs</p> <p>Workaround: There is no workaround. The CPE needs to be rebooted</p>
CSCdp78185	<p>cbos: High PPP memory utilization reported by Show Proc</p> <p>Description : Repeat PPP authentication failures will cause the CPE to run out of memory. This occurs when "ppp restart" is enabled and the PPP credentials don't match between the CPE and CO side.</p> <p>Condition : Memory utilization will be consumed by the PPP process. This affects the 67x</p> <p>Workaround: Verify that the PPP username and password match the CO side.</p>
CSCdp81544	<p>cbos:Cant pass traffic with NAT enabled in Bridged Mode (ppp/rfc)</p> <p>Description : For bridging over RFC1483 or bridging over PPP, traffic between the CPE and the CO will not work unless NAT is Disabled. NAT is not designed to work on a bridged-connection.</p> <p>Condition : No traffic flow until the NAT is disabled. This affects the 67x</p> <p>Workaround: Disable NAT. NAT is disabled by default.</p>
CSCdp56726	<p>CPE hangs when different platforms image is sent via Xmodem</p> <p>Description : Xmodem download using other 6xx image may hang the CPE or place the CPE into the monitor mode once the CPE is rebooted after the Xmodem download.</p> <p>Condition : This may happen only if the image is incorrect.</p> <p>Workaround: Make sure the image to be downloaded is for the correct platform.</p>
CSCdp56047	<p>cbos: eth0 int up/down event does not generate syslog msg</p> <p>Description : The ethernet0 interface state is not logged in the syslog server when the port is disabled from the CLI. This affects the 67x CPE.</p> <p>Workaround: None</p>
CSCdp67889	<p>cbos: rip v2 md5 authentication is not working</p> <p>Description : RIP updates originated from the CPE side are not validated on the remote router.</p> <p>Workaround: There is no workaround. MD5 authentication should be disabled.</p>
CSCdp70210	<p>cbos: sh snmp shows unrelated messages. c675</p> <p>Description : Obtaining SNMP state show incorrect data via show snmp cli cmd</p> <p>Condition : No traffic flow until the NAT is disabled. This affects the 67x</p> <p>Workaround: Use "show run" or "debug SNMP" to view the SNMP information.</p>

Table 9 *Open Issues for CBOS Release 2.3.0*

ID Number	Description
CSCdp87640	<p>cbos:Cannot change pool size after learn is disabled</p> <p>Description : The DHCP server pool 0 size cannot be changed after disabling DHCP server learn.</p> <p>Condition : After the DHCP server learn is disabled and the DHCP server pool 0 size is manually changed, the new pool is not written in the running configuration or NVRAM. This affects the 6xx CPE.</p> <p>Workaround: Using the SET NVRAM DELETE cmd to remove the pool 0 size from the running configuration.</p>
CSCdp67457	<p>cbos:rip v2 does not receive routes from neighbors</p> <p>Description:When rip v2 is configured on the cpe and the remote neighbor, routes are not shown in the routing table locally but in the remote table. CPE sends updates in broadcast but fails to receive the updates from the neighbor.</p> <p>Condition:When rip v2 is configured on an interface.</p> <p>Workaround:None.</p>

Information from Previous Releases

The following new features are supported by CBOS Release 2.2.0. See the *Release Notes for Cisco Broadband Operating System Release 2.2.0* for additional information.

- XDMCP protocol for NAT
- Wildcard static NAT entries
- IPCP for static NAT entries
- VIP interfaces for NAT
- IGMP Proxies for NAT and PAT
- End-to-end pinging for OAM loopback cells
- Error log enhancements
- Display for negotiated Ethernet speed
- Exec login null password filtering
- In-band message reporting
- CBOS modifications for DOH compatibility
- DHCP Server duplicate address timer
- DHCP lease enhancements
- CHAP support
- VC Priority Queuing
- TFTP Clients
- Reboot timer
- Expanded exec level capabilities

- SNMP community names support

Related Documentation

Use these release notes in conjunction with these documents:

- *Cisco Broadband Operating System User's Guide*
- *Cisco 627 ADSL Router Installation and Operation Guide*
- *Cisco 633 ADSL Router 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*
- *Cisco 677 ADSL Router Installation and Operation Guide*
- *Cisco 678 ADSL Router Installation and Operation Guide*

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

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 CCO 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 product 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.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. 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

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

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/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users 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.

