Cisco Broadband Operating System 2.4.3.b Release Notes

January 25, 2002

These release notes describe new features and resolved and open issues for the Cisco Broadband Operating System (CBOS) Release 2.4.3b. Please refer to previous release notes for specific information concerning past releases.

For more detailed information about the information in these release notes, refer to the "Obtaining Documentation" section on page 8. Information about electronic documentation can be found in the "Cisco.com" section on page 9.

Contents

These release notes provide the following information:

CISCO SYSTEMS

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

Related Documentation

Use these release notes in conjunction with these documents:

- *Cisco 600 Series Installation and Operation Guide*
- *Cisco CPE Commander User Guide*
- *Cisco Data Connection Manager (CDCM) User Guide*
- *Cisco Broadband Operating System Release 2.4 User Guide.*
- *Cisco Broadband Operating System 2.3.5 Release Notes*
- *Cisco Broadband Operating System 2.3.9 Release Notes*
- *Cisco Broadband Operating System 2.4.1 Release Notes*
- Cisco *Broadband Operating System 2.4.2 Release Notes*
- Cisco *Broadband Operating System 2.4.2.b Release Notes*
- Cisco *Broadband Operating System 2.4.3 Release Notes*

Note There is important information in the *Cisco Broadband Operating System 2.4.3 Release Notes* that also applies to this release.

Cisco Broadband Operating System Release 2.4.3.b

This release of CBOS 2.4.3.b contains a fix for DSL modems which connect to a digital off-hook (DOH) DSLAM and do not have DOH enabled.

Caveats

The Cisco Commander software must not be running when you install CBOS 2.4.3.b.

This software starts out with the web server disabled (IP Socket 80 is closed). If you need the CPE web server enabled, you must change this setting in the configuration after the upgrade is completed.

TFTP server functionality is disabled by default on the CPE. If you have not manually enabled it, you must know your enable and exec passwords to install this software.

Caution Do not change anything else while making these changes; doing so can cause loss of connectivity or data.

Available Images

The following is the list of images that can be downloaded to the CPE.

Note You must use the image specific to your CPE device. If you try to use an image for a different device, you will be unable to connect to your service provider.

- 627 full-rate
- 627 g.lite
- 633
- 673
- 675
- 677 full-rate
- 677 g.lite
- 677i
- 678 cap
- 678 dmt full-rate
- 678 dmt g.lite

To find the image that a 677 or 678 CPE is running, from the CBOS command line, enter:

show version

For more information on upgrading please see the Release Notes for the previous releases of CBOS, and the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/600-v242?param=case3

Configuring VIP Outside with CBOS 2.4.3.b

With CBOS 2.4.3.b, the VIP network has its own Outside Global IP address. Traffic sourced from the VIP Outside network to the Inside network requires a static NAT entry specifying the VIP Outside Global IP address.

Note The VIP configuration of public or private addresses behind a 600 series CPE still limits the user to the one outside NAT address for WAN access.

To set a VIP network to Outside, add the following command:

set int vip*x* outside

where x is a value ranging from 0 to 2.

To set the VIP Outside Global IP address add the following command:

set interface vipx **ip** *address*

To allow traffic from the VIP Outside network to access the Inside network, add the following command:

set nat entry add *inside_IP_address inside_port VIP_Outside_IP Outside_port protocol*

Example Configuration

The following is an example configuration for a CPE 675:

```
675-rc4#show config
[[ CBOS = Section Start ]]
NSOS Prompt = 675-rc4
NSOS 1483 Routing = enabled
NSOS MD5 Enable Password =
C64100007F160000812700006C44000046D96F11BD49778827656
8D7C2CDE806
NSOS MD5 Root Password =
8D030000215900000028000073320000F0247C9D8312335A0F18738
AB2509E97
NSOS MD5 Commander Password = E7061E2A3FC26E5E101400453E424DFC
NSOS Virtual IP Address = 00, 33.1.1.1
NSOS Virtual IP Address = 01, 44.1.1.1
[[ IP Routing = Section Start ]]
IP Port Address = 00, 11.1.1.1
IP NAT Outside IP = 22.1.1.1
IP NAT = enabled
IP NAT VIP Port Side = 01, inside
IP NAT Entry = 44.1.1.2, 69, 31.1.1.1, 69, udp;11.1.1.2, 23, 21.1.1.1, 23,
tcp;
[[ DHCP = Section Start ]]
DHCP Server Pool IP = 00, 11.1.1.2
DHCP Server Pool Gateway = 00, 11.1.1.1
DHCP Server Pool DNS = 00, 171.71.193.20
[[ TFTP = Section Start ]]
TFTP = enabled

675-rc4#show nat

NAT is currently enabled

Port      Network       Global
eth0      Inside
wan0-0    Outside       22.1.1.1
vip0      Outside       33.1.1.1
vip1      Inside
vip2      Outside

     Local IP : Port      Global IP : Port      Timer Flags    Proto
Interface
      11.1.1.2:23           21.1.1.1:23          0    0x00041  tcp   eth0
      44.1.1.2:69           31.1.1.1:69          0    0x00041  udp   vip1

675-rc4#show int
        IP Address        Mask
eth0      11.1.1.1          255.255.255.0

vip0      33.1.1.1          255.255.255.0

vip1      44.1.1.1          255.255.255.0
```

```
vip2        0.0.0.0                255.255.255.0

wan0        Physical Port: Trained

            Dest IP Address    Mask
wan0-0      0.0.0.0            255.255.255.255
```

Resolved Issues in CBOS Release 2.4.3.b

The following issues can be resolved by installing Release 2.4.3.b of CBOS.

- CSCdv609912

  CBOS2.4.3: CPE training process changed and no longer works with DOH DSLAMS.

Known Issues in CBOS Release 2.4.3.b

This section lists open issues for CBOS 2.4.3.b

> **Note** The following known issues also existed in CBOS 2.4.2, CBOS 2.4.2.b, and CBOS 2.4.3. They are listed here for your convenience.

- CSCdv75882

  Symptom:

  All traffic, which is sourced from a remote network and destined for ethernet0 (inbound), will be dropped.

  Condition:

  This symptom occurs when NAT is enabled.

  Workaround:

  There is no workaround.

- CSCdu20238

  When going from RFC1483 routing or PPP routing to RFC1483 bridging, the 67x CPE receiving autoconfiguration information may not use the VPI/VCI information sent via autoconfiguration. Instead, it might use the default VPI/VCI of 1/1.

  Condition:

  This problem occurs intermittently when switching from RFC1483 routing or PPP routing to RFC1483 bridging. It might also occur when doing other types of service changes.

  Workaround:

  The workaround is to completely remove the previous service profile before adding a new service profile of a different type. Do not add the second service profile before you delete the first.

- CSCdp67889

  Symptom:

  MD5 authentication does not work when using RIP v2.

  Condition:

  This symptom occurs when using MD5 authentication with RIP v2.

  Workaround:

  Use another form of authentication with RIP v2.

- CSCdt86398

  Symptom:

  When PPP is enabled on a wan0-1 interface requiring a negotiated address, PPP-IPCP still attempts negotiation without the command **set int wan0-1 ipcp 0.0.0.0** being set.

  Condition:

  This symptom occurs when using PPP on an interface that requires a negotiated address.

  Workaround:

  There is no workaround.

- CSCdt86505

  Symptom:

  RIPV1 broadcasts are forwarded by the CPE out of wan0-0 even though forwarding is disabled.

  Condition:

  When a RipV1 speaking device is placed behind the Eth0 interface on a CPE, the broadcast updated will be propagated out the Wan0-0 interface even if broadcast forwarding is disabled.

  Workaround:

  There is no workaround.

- CSCdt87674

  Symptom:

  RIPv2 multicast updates ar propagated out the Wan0-0 interface when a RIPv2 speaking device is placed on the Eth0 interface of the CPE and multicast forwarding is disabled.

  Condition:

  A CPE running RipV2 with a device on the Eth0 interface allows the multicast routing updates to be propagated out the wan0-0 interface even if multicast forwarding is disabled.

  Workaround:

  There is no workaround.

- CSCdt87979

  Symptom:

  Any routes learned via RIPv2 on the CPE's Eth0 interface are not propagated out any wan0-*x* interfaces.

  Condition:

  The issue occurs when the CPE is configured with multiple wan0-x interfaces using RIPv2.

Workaround:

There is no workaround.

- CSCdt88021

    Symptom:

    Multicast RipV2 updates are not propagated out wan0-*x* (where x is 1 through 7) when multicast forwarding is enabled.

    Condition:

    A CPE with multicast forwarding enabled will not forward the multicast packets out any interface other than wan0-0.

    Workaround:

    There is no workaround.

- CSCdt89643

    Symptom:

    Commands in the Running Configuration that have not been written to NVRAM are lost when upgrading to CBOS release 2.4.2 or higher.

    Condition:

    This issue occurs when upgrading to CBOS release 2.4.2 or higher.

    Workaround:

    Before you upgrade, make sure your running configuration and NVRAM configuration match.

⚠

Caution   Before you upgrade to CBOS release 2.4.2 or higher, make sure your running configuration and NVRAM configuration match. Otherwise, any running config commands that have not been saved to NVRAM are lost.

- CSCdt94627

    Symptom:

    Some features of NetMeeting do not operate correctly with NAT enabled.

    Condition:

    Table 1 shows how NetMeeting works with CBOS 242, with and without NAT.

Table 1   *Net Meeting Features*

Features/CPE Setup	Initiated inside with NAT	Initiated outside with NAT	Initiated inside without NAT	Initiated outside without NAT
video	yes	yes	yes	yes
voice	yes	yes	yes	yes
chat	yes	no	yes	yes
whiteboard	yes	no	yes	yes
file transfer	yes	no	yes	yes

Table 1   Net Meeting Features (continued)

Features/CPE Setup	Initiated inside with NAT	Initiated outside with NAT	Initiated inside without NAT	Initiated outside without NAT
desktop sharing	yes	no	yes	yes
desktop remote control	yes	no	yes	yes

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 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 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, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
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.

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