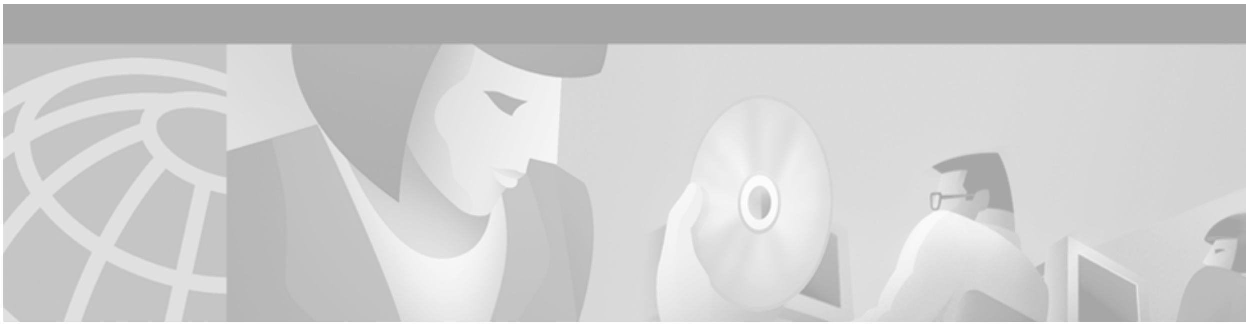

Release Notes for Cisco Application and Content Networking Software, Release 4.1.3

June 06, 2002

Note: The most current Cisco documentation for released products is available at Cisco.com at http://www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback.

Contents

These release notes contain information about ACNS software, Release 4.1.3. These release notes describe the following topics:

Cisco Systems

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

Introduction

These release notes describe new information, caveats, and other important information regarding ACNS software, Release 4.1.3.

New and Changed Information

This section lists new or changed information in ACNS software, Release 4.1.3.

New CLI Command

The following CLI command has been added:

transaction-logs log-windows-domain

If your device is configured for NT LAN Manager (NTLM) authentication and uses Apache Common Log Format, the **transaction-logs log-windows-domain** command records the Windows domain name and username in the "authenticated username" field of the transaction log. If the domain name is available, both the domain name and the username are recorded in the "authenticated username" field, in the form domain\username. If only the username is available, only the username is recorded in the "authenticated username" field. If neither a domain name nor a username is available a "-" (hyphen) is recorded in the field.

Use the **no** form of the command to negate logging NTLM parameters in Apache Common Log Format.

no transaction-logs log-windows-domain

Caveats

This section lists and describes caveats that were resolved in ACNS software, Release 4.1.3, and caveats that are still open in this release.

Caveats describe unexpected behavior in ACNS software, Release 4.1.3. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Resolved Caveats - Release 4.1.3

- CSCdw51456

  Although the **copy disk ftp** command functions normally, it does not display any output data.
- CSCdw62458

  HTTPS performance over the Content Engine is much slower than without the Content Engine.
- CSCdw64167

  The CPU usage data shown with the **show statistics http usage** command is different from the data shown with the **show processes cpu** command.

- CSCdw65996

  SNMP packets with long object identifiers (OID) cause the SNMP agent to automatically reboot. The SNMP agent code was not checking for maximum length of the OID, thus causing the memory corruption. This caveat was resolved in ACNS software, Release 4.1.1.

- CSCdw68848

  When you try to downgrade from ACNS software Release 4.1 to E-CDN Release 3.x software on a system where the **disk config** command has been used to assign non-ecdnfs storage, the downgrade sometimes fails.

- CSCdw71953

  The HTTP proxy stops accepting new requests.

- CSCdw75147

  TACACS authentication does not work when authenticating for Secure Shell (SSH) sessions.

- CSCdw76569

  The Cache application unexpectedly reloads on a CE-7320 platform when this platform is overstressed.

- CSCdw77632

  The system slows when using rules that do regular expression (regex) matching.

- CSCdw77773

  The HTTP proxy unexpectedly reloads.

- CSCdw77966

  The **cache clear** command sometimes does not finish. Instead, a message appears that includes the text “verifier error.” Cache service is not interrupted. However, cfs volumes may have been cleared, while other volumes may not have been cleared. The **show statistics cfs** command shows which volumes were cleared (low count of bytes in use) and which were not cleared (high or unchanged count of bytes in use).

- CSCdx04080

  ACNS 4.x with SSH enabled. Potential problems are corrected with zlib compression software relating to Cisco Security Advisory: Vulnerability in the zlib Compression Library Revision 1.0. Go to the following URL for more information:
  http://www.cisco.com/warp/customer/707/zlib-double-free.shtml

- CSCin03870

  The web server unexpectedly reloads when transitioning from an SNMP page to an SNMPv3 GUI page.

Open Caveats - ACNS Software Release 4.1.3

- CSCdu36845

  Symptom: The TV-out GUI allows a non-BMP file type to be used as an overlay image. For example, if an .mpeg file larger than 64 KB is used as the overlay image, the system goes into a loop.

  Condition: This symptom occurs on a CE-507 AV or CE-560 AV running ACNS 4.0 or later software.

Workaround: Do not use a non-BMP file type as an overlay image. To resolve problems caused by using a non-BMP file as an overlay image, remove the TV-STATUS record on the Content Engine. You can do this accessing the box. To do this, go to the following URL:

http://<CE IP>/cgi/box

where <CE IP> is the Content engine address.

1. Choose **ShowLib** and enter T**V-STATUS** in the Table regex field.

2. Click **Show**, choose **Record**, and click **Delete checked records**.

- CSCdu79580

  Symptom: If you repeatedly click NEXT (10–15 times) from the GUI or the API while the playlist is in PLAY mode, the video server may pause indefinitely. The video monitor flickers for awhile as it attempts to play the next file and then it pauses indefinitely.

  Condition: This symptom occurs on systems running the E-CDN application, Release 3.0 and 4.0.

  Workaround: The E-CDN application must stopped and restarted to clear the error condition. Follow these steps:

  1. Wait for an automatic restart; this may take up to 60 minutes (all versions).

  2. Disable and then enable the E-CDN application.

  3. Reboot the system (all versions).

  4) Use Telnet to access the system and use the **vbox stop** and the **vbox start** commands. (Version 3.0).

  This pause *only* occurs when you click the NEXT button several times a second, because the problem is the frequency of clicking and not the actual click count. You can avoid the pause by clicking NEXT at a slower pace, and pausing for a second or two between clicks.

- CSCdv29357

  Symptom: During the playback of some MPEG-2 files using TV-out, the video decode freezes at some position in the file while the audio decode continues. Repeated playback shows that the video freeze occurs at the same position. In some extreme cases, the problem occurs on the first frame of video, causing playback to fail entirely.

  Condition: This symptom occurs on systems running any Enterprise-CDN or ACNS software version. The hardware is the CE-507AV-CDN or CE-560AV-CDN, manufactured with the Vela CineView 2083 MPEG decoder card.

  Workaround: The problem occurs with MPEG-2 files encoded at a variable bit rate (VBR).The hardware decoder interprets some sequences as an error, and stops the decode. We recommend that MPEG-2 files encoded for TV-out use constant bit rate (CBR) to avoid this problem. File exhibiting this behavior should be re-encoded.

  In the extreme case noted above, the TV-STATUS record may need to be removed to recover playback operation. This is only if the VBR file cannot be removed from the playlist through the TV Controller GUI. Go to the following URL:

  http://<CE IP>/cgi/box

  where <CE IP> is the Content Engine IP address.

  1. Choose **ShowLib** and enter 'T**V-STATUS** in the Table regex field.

  2) Click **Show**, choose **Record**, and click **Delete checked records**.

- CSCdw33364

  Symptom: Occasionally, the user cannot access the Realserver and receives the following error message:

  ```
  Server has reached its capacity
  ```

  Condition: Run only one RealServer client to test the RealServer live splitting through the Content Engine. You must run the client for two hours.

  Then try to start second RealServer client. You may sometimes see the following message:

  ```
  Server have reaches it capacity
  ```

  and you may not be able to play any files from the Content Engine. If you check the publisher RealServer, you see that the current number of connections is 104, but in fact there is only one RealServer client receiving the live stream.

  Work around: Restarting the publisher and subscriber Real Server solves the problem.This caveat has been fixed by Real Networks in their next release.

- CSCdw53913

  Symptom: The user may see the following error message in the syslog.txt:

  ```
  Jan 20 18:30:34 bfc9000 Diamond: KERNEL: assertion (req->sk == NULL) failed
  at tcp_ipv4.c(780):tcp_v4_search_req
  ```

  Condition: This error message occurs only on the CE-7320 when Web Cache Communication Protocol (WCCP) is enabled. It does not seem to have any negative effect on the system function. WCCP continues to work as expected.

  Workaround: No workaround is needed.

- CSCdw68467

  Symptom: When the **copy startup-config running-config** command is used, the shell prompt is not returned.

  Condition: If the **copy startup-config running-config** command is used when the CLI_INTERACTIVE flag is set, it triggers the execution of
  /diamond/bin/config (generated from bfc/systems/cli/exec/src).

  This **/diamond/bin/ config** command executes the content in the startup configuration line by line. Certain **config** commands prompt the user and wait for the user's response, causing the **copy** command to pause indefinitely (stdout and stderr have been redirected) because there is no user response to the prompt.

  This condition does not occur when the system boots up, because the CLI_INTERACTIVE flag is not set during bootup.

  Those configuration commands that need user interaction call the function GetCLIMode(), which determines whether or not to enter interactive mode.

  Workaround: If the **copy startup-config running-config** command pauses indefinitely, press **Enter** as needed, until the command has finished executing.

- CSCdw71468

  Symptom: When the user programmatically imports content into a channel on the Content Distribution Manager, if the status return field is HTML or MX (E-CDN application proprietary format), then the status is not returned.

  Condition: This occurs in ACNS software, Release 4.1.3.

  Workaround: There is no known workaround.

- CSCdw73329

  Symptom: The Content Engine may pause indefinitely during bootup when it is physically connected to a console server port that does not have an active session running on it to clear out the console messages.

  Condition: A caveat in the console server causes spurious characters to be sent to the Content Engine console when the console server buffer overflows.

  Workaround: Open an active session on the console port to clear out the console messages and to avoid overflow of console server buffers.

- CSCdw75439

  Symptom: The Storage Array 6 is not recognized by the Content Engine.

  Condition: One defective disk in the Storage Array 6 causes the entire Storage Array to automatically reboot, and the Content Engine recognizes only the internal drives. The LED on the defective drive flickers once every second. The Storage Array is not recognized and does not appear in the Linux prompt **df** command display.

  Workaround: Removing the defective drive allows the remaining drives to become operational and be recognized by the Content Engine.

- CSCdw76156

  Problem: Removing a Storage Array 6 that had the only sysfs partition results in a system with two disks allocated only to cfs and ecdnfs.

  Condition: This happens anytime the sysfs partition is not located on drive0.

  Workaround: Allocate sysfs to drive0, which can be done by using the **disk config** command.

- CSCdw77517

  Symptom: E-CDN CEs and clients deployed behind the same NAT-based firewall are not recognized as such by a CDM outside the firewall. Requests made from clients or CEs inside the firewall can result in the following:

  a. Requests may not be redirected to a primary CE inside the firewall for further processing

  b. Requests may be redirected to a primary CE inside the firewall that cannot redirect the request to the appropriate CE.

  This can occur if the outbound NAT addresses of the firewall do not have the same Class C network address (That is, they do not share the same first three octets of their IP addresses).

  Condition: Present in all E-CDN and ACNS releases.

  Workaround: There is no workaround.

- CSCdw82157

  Symptom: The **disk configure** command does not use the remaining (unused) space on disk00 for mediafs storage.

  Condition: After upgrading from ACNS 4.0 to ACNS 4.1 beta (4.1.0b14), disk00 has 12GB of “free” space. This space cannot be used for mediafs storage, because ACNS software does not support the **disk partition** command to manually create a disk00/03 partition. The **disk configure** command does not touch disk00 at all, so the result is lost disk space. This means that not all purchased disk space is usable.

  Workaround: There is no workaround.

- CSCdw90323

  Problem: The Content Engine does not add a bypass entry for the Client IP address-Dest IP address pair if the connection times out.

  Condition: Transparent error handling might not have been enabled.

  Workaround: Enable transparent error-handling by issuing the **error-handling transparent** command.

- CSCdw91108

  Symptom: The Content Engine does not accept requests on secondary addresses.

  Condition: If a secondary address (alias) is configured for an interface and a request is made to the Content Engine in proxy mode using the secondary address, the request is not processed. Instead the connection is closed.

  Workaround: Configure the secondary IP address to be an external IP address as follows:

  ```
  CE(Config)#external-ip <ip-address>
  ```

  where <*ip-address*> is the secondary IP address of an interface to use as the proxy IP address.

- CSCdx00361

  Symptom: When multiple plug-ins (for example, Content Optimization and SmartFilter) are enabled at the same time, the caching process automatically reboots.

  Condition: An HTTP request is sent to the Content Engine if multiple plug-ins are enabled.

  Workaround: There is no known workaround.

  Note This problem only affects the Content Optimization Engine product because it is the only product that is capable of accepting multiple plug-ins. The base Content Engine configuration has only the SmartFilter plug-in and is not affected by this problem.

- CSCdx03843

  Symptom: All traffic to the Content Engine is bypassed after the following CLI command is issued:

  ```
  show wccp flows web-cache detail
  ```

  Condition: This symptom occurs intermittently on systems running ACNS software.

  Workaround: Test for this condition by repeating the CLI command and viewing the output. If the flags field is blank for all buckets, disable the service and enable it again.

- CSCdx04092

  Symptom: Using an embedded Windows Media Player object in an HTML page to point to an ASX file that contains the WMT Play URL from the CDM Previewer page for an imported ASF file does not work. You receive an error message saying that the filename is invalid.

  Condition: This symptom only occurs when you are using the embedded Windows Media Player object in an HTML page. Does not occur if you are using the full Windows Media Player.

  Workaround: Use the Windows Media Player (not the embedded object). Or, if you must use the embedded player, have it point directly to the WMT Play URL instead of an ASX file.

- CSCdx04156

  Symptom: The Pluggable Authentication Module (PAM) creates unnecessary system log entries during user login.

Condition: This symptom occurs during user login on systems running ACNS software.

Workaround: There is no known workaround.

- CSCdx04177

  Symptom: You cannot use .sami (Synchronized Accessible Media Interchange) files with WMT playing from the Content Distribution Manager or Content Engine.

  Workaround: There is no known workaround.

- CSCdx13400

  Symptom: If the media player tries to play a clip through the HTTP protocol (the user chooses to only use the HTTP protocol as the transport), it will not work.

  Condition: This symptom occurs if the user has two Content Engines, one internal (CE1) and the other upstream (CE2), and if the user issues the **http proxy outgoing host** command on CE1 to point to CE2, and CE2 is the only way to reach outside the CDN through the HTTP protocol. Basically, WMT over HTTP does not work with the **http proxy outgoing host** command, and it goes directly to the origin server with going to the CE2 first.

  Workaround: There is no known workaround.

- CSCdx18600

  Symptom: The output from the **show clock** CLI command may not display the correct time zone name.

  Conditions: This symptom occurs when the **show clock** CLI command is used on systems running ACNS software.

  Workaround: There is no known workaround.

- CSCdx20175

  Symptom: When you try to use the **cfs clear** command, the following error results:

  ```
  umhscache#cfs clear disk00/03 force
  unable to create lock file
  ```

  Workaround: Use the **clear cache** command. This problem is likely caused by a full RAM disk.

- CSCdx23688

  Symptom: When logging in as a TACACS user, the user does not appear in the user list.

  Workaround: There is no known workaround.

- CSCdx28999

  Symptom: “Permission denied” messages are received when you import a folder using FTP drag and drop with Netscape 4.7. Subsequent attempts to import files using FTP drag and drop fail, and “unable to find the file or directory” messages is displayed.

  Condition: This symptom occurs with ACNS 4.1.x software.

  Workaround: Use a different browser (Internet Explorer) if you need to import folders using FTP drag and drop. If you need to use Netscape 4.7, exiting and restarting the browser will eliminate the subsequent “unable to find the file or directory” errors.

- CSCds66386

  Symptom: Changes to the network settings of a Content Engine or a Content Router (including DNS settings, whether or not an HTTP proxy is configured for use, and IP address information) made through the CDM user interface do not seem to have any effect.

Condition: The symptom occurs in Enterprise CDN 3.0 software.

Workaround: The device must be rebooted for these changes to take effect.

- CSCdx37512

  Symptom: The HTTP proxy keeps restarting.

  Problem: WCCP keeps restarting.

  Workaround: To work around this problem, follow these steps:

  1. Use the **no wccp enable** command to disable WCCP.

  2. Reload the device.

  3. Use the **wccp enable** command to reenable WCCP.

- CSCdx37517

  Symptom: This problem will not affect customers.

  Condition: The rtsp_proxy did a core dump when it tried to connect to the WCCP process. The WCCP module in the rtsp_proxy was not able to free all the resources cleanly.

  Workaround: No workaround is necessary. The rtsp_proxy will restart.

- CSCin06968

  Symptom: When using the proxy automatic configuration (.pac file) feature, the request for the proxy.pac file should not be forwarded to an upstream proxy device, even if an upstream proxy is configured.

  Conditions: This symptom occurs if the proxy automatic configuration feature is enabled and an outgoing proxy is configured.

  Workaround: Enter a no-proxy rule to prevent the proxy .pac requests from being forwarded to the upstream proxy.

- CSCin07452

  Symptom: The rule cache feature does not work when the pattern type is mime-type.

  Condition: This symptom can occur when the “Cache-Control: no-store” and “pragma: no-cache” headers come before the “Content-type:” header.

  Workaround: There is no known workaround.

- CSCin12268

  Symptom: The **show version** command in Release 4.1.3 Build b6, returns the version identifier `<unknown-version>`.

  ```
  Application and Content Networking Software (ACNS)
  Copyright (c) 1999-2002 by Cisco Systems, Inc.
  Application and Content Networking Software Release 4.1.3 (build b6 May 1 2002)
  Version:ce590-<unknown-version>
  Compiled 16:06:41 May 1 2002 by bbalagot
  Compile Time Options:PP
  System was restarted on Fri Jun 21 17:12:50 2002.
  The system has been up for 46 minutes, 2 seconds.
  ```

  Condition: The Version field is used by the Software Image Manager (SWIM) application in Resource Manager Essentials (RME) software of CiscoWorks 2000 to identify the running version of ACNS software on the Content Engine. SWIM cannot be used with Release 4.1.3 Build b6.

  Workaround: There is no workaround for Release 4.1.3 Build b6.

Related Documentation

Your product shipped with a minimal set of printed documentation, as well as a Documentation CD. The printed documentation provides enough information for you to install and initially configure your product. The CD contains additional product documentation (user guides, configuration manuals, and so forth), which you can access and print out.

Product Documentation Set

In addition to these release notes, the product documentation set includes:

- *Documentation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Content Delivery Networking Products Getting Started Guide*

Refer to the *Documentation Guide* for a complete documentation roadmap and URL documentation links for this product.

Hardware Documentation

- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Software Documentation

- *Cisco Application and Content Networking Software Caching Configuration Guide*
- *Cisco Application and Content Networking Software Command Reference*
- *Cisco Application and Content Networking Software E-CDN Administrator's Guide*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.0.2*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

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:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

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