



Release Notes for Cisco ACNS Software, Release 4.2.7

February 24, 2003



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 4.2.7. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Additional Hardware Supported, page 3](#)
- [Caveats, page 4](#)
- [Documentation Updates, page 9](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Introduction

These release notes describe new features, supported hardware, and open and resolved caveats regarding ACNS software, Release 4.2.7.

New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 4.2.7. These features include the following:

- [Adding HTTP Request Methods](#)
- [Windows Media Player Version 9.0](#)

Adding HTTP Request Methods

Content Engines accept or reject a Hypertext Transport Protocol (HTTP) request depending on whether the request method is supported. In ACNS software, HTTP request methods are categorized as supported and unsupported. HTTP 1.1 request methods (for example, GET, HEAD, or POST) are supported by default. Nonstandard request methods, such as Web-Based Distributed Authoring and Versioning (WebDAV) are not. In previous releases of ACNS software, users were unable to add or delete HTTP request methods using a CLI command and had to ask Cisco to perform this function. ACNS software, Release 4.2.7 adds the **http add-method** global configuration command to let you add HTTP request methods to the list of those supported by the Content Engine, and the **no** version of this command, **no http add-method** that lets you remove a method from the list.

The following example adds the WebDAV REPORT method to the list of supported methods.

```
ContentEngine(config)# http add-method REPORT
ContentEngine(config)#
```

You can run the **show http methods EXEC** command to display a list of supported and unsupported HTTP request methods. In the **show http methods** command output, request methods supported by default appear in parentheses.

This is an example of the **show http methods** command:

```
ContentEngine# show http methods

Request headers supported for HTTP:
-----
(Default methods shown in-between braces)

(GET), (POST), (HEAD), (PUT), (TRACE)
(DELETE), (OPTIONS), (CONNECT), (PURGE), (NETHCMD)
(PROPFIND), (PROPPATCH), (MKCOL), (COPY), (DELETE)
(MOVE), (LOCK), (UNLOCK), (BIND), (BMOVE)
(BCOPY), (BDELETE), (BPROPFIND), (BPROPPATCH), (SEARCH)
(SUBSCRIBE), (UNSUBSCRIBE), (POLL), (SUBSCRIPTIONS), (ACL)
(NOTIFY), (INVOKE), REPORT

Unsupported Request Methods Hit :
-----
(Sorted in more recently used order)

ContentEngine#
```

REPORT is listed as the last entry in the output. It does not appear in parentheses, as REPORT is not a default method.

A description of WebDAV and WebDAV methods is available as IETF RFC 2518, *HTTP Extensions for Distributed Authoring—WEBDAV*.

**Note**

When the Content Engine receives an HTTP request from a client using a method not supported, ACNS software adds the method to the list of unsupported methods and returns an error to the client. You can add any method not supported to the list of supported methods.

Windows Media Player Version 9.0

ACNS software, Release 4.2.7 supports Windows Media Player version 9.0. The support is limited to Windows Media Player, and does not include other components in the Windows Media Technologies 9.0 series suite.

Windows Media Player version 9.00.00.2980 has been tested on ACNS software, Release 4.2.7. We have not tested later versions of Windows Media Player 9.0 on ACNS software, Release 4.2.7. You can contact Content Networking Business Unit (CNBU) product marketing to learn about support for later versions of Windows Media Player 9.0.

**Note**

Windows Media Player 9.0 bypasses the proxy and serves the request from the origin server when the proxy server fails to serve a request that uses MMS-over-HTTP as the protocol. Previous versions of Windows Media Player (versions 6.4 and 7.0) did not support this feature.

Typically, proxy servers fail to serve a request if:

- The requested media file exceeds the configured values in the Content Engine (bandwidth, maximum number of sessions, and maximum bit rate)
- The URL fails to pass the rules or URL filter configured in the Content Engine
- The proxy server is down

Additional Hardware Supported

ACNS software, Release 4.2.7 supports the Content Engine Network Module for the 2600, 3600, and 3700 series branch office routers. The following table lists the supported branch office router part numbers and descriptions.

Part Number	Description
NM-CE-BP-20G	Content Engine NM-Basic Perf-20 GB
NM-CE-BP-40G	Content Engine NM-Basic Perf-40 GB
NM-CE-BP-SCSI	Content Engine NM-Basic Perf-SCSI adapter
EM-CE-20G=	Expansion Module, 20-GB IDE, field upgrade
EM-CE-40G=	Expansion Module, 40-GB IDE, field upgrade
EM-CE-SCSI=	Expansion Module, SCSI controller, field upgrade

Part Number	Description
MEM-CE-256U512D	512-MB DRAM factory upgrade for NM-CE-BP
MEM-CE-256D=	256-MB DRAM field upgrade
MEM-256CF-4.2.K9=	256-MB Compact Flash with ACNS software, 4.2 recovery image, 3 DES (Data Encryption Standard)

Caveats

This section lists and describes caveats that are still open in the ACNS software, Release 4.2.7, and caveats that were resolved in this release. Caveats describe unexpected behavior in ACNS software, Release 4.2.7. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats - ACNS Software, Release 4.2.7

- CSCdw84848**

Symptom: The contents of a file whose name exceeds 215 characters cannot be imported.

Condition: This occurs on a Content Distribution Manager 4630 or 4650 running ACNS software, Release 4.2.

Workaround: Rename filenames so that they are shorter than 215 characters.
- CSCdy02581**

Symptom: WCCP bypass does not function properly when bypassing packets of large size from the client. Therefore, the client never receives an acknowledgment from the server for the data sent.

Condition: This problem occurs when the Content Engine bypasses the connection and the server advertises a maximum segment size (MSS) of 1460 bytes.

Workaround: There is no known workaround.
- CSCdy03638**

Symptom: A banner message cannot be set in Content Engines running ACNS software, Release 4.x.

Workaround: There is no known workaround.
- CSCdy16548**

Symptom: When you use ACNS software to verify Windows NT LAN Manager (NTLM)-supplied passwords on a Windows server, if the password is longer than 14 characters, the authentication fails.

Condition: When you enter a password that is longer than 14 characters on a Windows 2000 or Windows XP system, authentication fails.

Workaround: Do not use an NTLM user password that is longer than 14 characters.

- CSCdy68833
Symptom: A core dump is seen under /local1/core_dir for Real-Time Streaming Protocol (RSTP) and the video server.
Condition: This core dump is generated by the video server when the E-CDN software is enabled in a CE-507.
Workaround: There is no known workaround.
- CSCdy74268
Symptom: The CE-5xxAV stops playing, and TV output cannot be controlled.
Condition: This symptom occurs after the user clicks the Next button on the Content Engine home page several times in a short period (about 2 seconds).
Workaround: There is no known workaround.
- CSCdy76795
Symptom: The CE-5xxAV runs 9 hours ahead of Japan Standard Time (JST) in the playlist review when the time zone is set to JST (Asia/Tokyo, GMT + 9 hours). In other words, the time is an additional 9 hours ahead of GMT.
Condition: This symptom appears when you change time zones for the Content Engine.
Workaround: There is no known workaround.
- CSCdy80020
Symptom: Occasionally, when a CE-507 is being upgraded from E-CDN software, Release 3.0.3 to ACNS software, Release 4.2.1, it requires the rescue image after an upgrade is attempted.
Workaround: Click the Update Storage Capacity button on the Content Engine System page in the Content Distribution Manager GUI to be sure that you have at least 1.2 GB of space not assigned to channels. You can also reboot the Content Engine from the Content Engine System page in the Content Distribution Manager GUI and wait 15 minutes. This ensures that the Content Engine is stable and ready for upgrade.
- CSCdy84704
Symptom: After the time zone is changed to another region, the system time (which is shown in the Identification window on the Content Distribution Manager GUI) does not change.
Workaround: There is no known workaround.
- CSCdz01265
Symptom: The Content Engine is not deleting orphaned contents if a subscribed channel is removed when that Content Engine is shut down.
Condition: This occurs in ACNS software, Release 4.2.1.
Workaround: There is no known workaround.
- CSCdz10104
Symptom: Importing a large number of files using FTP is not successful if the filenames do not have extensions. The import process proceeds normally until a few hundred files have been successfully imported. However, the import process stops after that.
Condition: This problem is observed when the content items or files do not have filename extensions (for example, specifying the filename as “123” instead of “123.gif”).
Workaround: There is no reliable workaround, although restarting the E-CDN application will restart the import process, but some files might be lost during the process.

- CSCdz56234
Symptom: The **ip domain-name** CLI command cannot be used to specify more than one domain.
Condition: This symptom is observed in a Content Engine using the E-CDN application in which the IP domain name configuration is overwritten with that specified in the E-CDN configuration.
Workaround: If the user needs multiple domain names to be set on the Content Engine, all related DNS settings must be made from the individual Content Engine and not from the Content Distribution Manager GUI.
- CSCsp01389
Symptom: The default start and stop times are those of the user's system device and not of the TV-out device. This is observed when the TV-out device is in a different time zone with a different date, month, or year.
Condition: This occurs in E-CDN software, Release 2.1 or later (including ACNS software, Release 4.x).
Workaround: There is no known workaround.

Resolved Caveats - ACNS Software, Release 4.2.7

- CSCdt62678
The software upgrade fails if the user clicks the Upgrade button before the upgrade files are replicated to the Content Engines.
- CSCdy35907
The reply code field in the HTTP transaction log does not accurately reflect the actual error condition. For many of the error conditions, the reply code field in the HTTP transaction log is not mapped to the corresponding error message.
- CSCdy58335
Rarely, in the case of stacked requests, the DNS count of outstanding queries grows continuously without limit.
- CSCdy71516
Importing files, using FTP, into the Content Engine from a Linux machine causes the following error message to be displayed on the console.

```
exiting on signal 11: Segmentation fault
```


This symptom occurs only when the username and password supplied in the Content Engine are longer than 31 characters. Also, a logging console needs to be enabled and the priority set to Debug to observe this condition.
- CSCdz03816
The WMT statistics display conflicting information in certain situations. In this case, the **show statistics wmt streamstat** command displays connections that are unaccounted for. This symptom might be observed when the Content Engine is fully loaded and WMT traffic is high.
- CSCdz23066
Third-party applications that support HTTP transaction statistics based on the Squid or Extended Squid HTTP transaction log file format report more cache misses than are actually caused by defects on the Content Engine.

- CSCdz37096

“File not found” errors are generated by remote servers when more than five live stream sessions are started at the same time.
- CSCdz49175

The date and time stamps in the HTTP transaction log are incorrect occasionally for a few entries. This condition is more likely to occur on Content Engine models with multiple processors, such as the CE-7320.
- CSCdz50695

When a Content Engine receives a “100 Continue” response after a POST request, it switches itself to the pipe-through mode and performs a two-way pipe-through between the server and the client. The server does not close the connection after serving the POST request. Therefore, the Content Engine does not process successive requests from the client and instead passes them directly to the server over the same connection. This symptom is observed in proxy mode because the browser uses HTTP 1.1 by default, which in turn uses a persistent connection.
- CSCdz50936

The read () function does not yield the desired results when used under extreme network conditions.
- CSCdz55182

The **memory-manual** command can be easily configured by typing **mem** in configuration mode, which causes memory resources for all applications to be set to zero by default. The command, when enabled, also causes NT LAN Manager (NTLM) to stop working.
- CSCdz56234

The **ip domain-name** CLI command cannot be used to specify more than one domain on a Content Engine using the E-CDN application.
- CSCdz57412

When the Microsoft Media Server’s (MMS) Windows Media Services is restarted and the Windows Media Player is playing a stream, the TCP connection between the MMS server and the Content Engine is disabled, although the Content Engine shows that the media player is still in a paused state. In other words, after the source of live stream is disconnected from the Content Engine, it takes about a minute for the Content Engine to disconnect from the Windows Media Player.
- CSCdz61728

The error number 0 appearing in the system logging (syslog) message incorrectly indicates that the disk is full. This symptom is observed in ACNS software, Release 4.2.3 and later.
- CSCdz62646

A core dump is generated by the Microsoft Media Server (MMS) when the **wmt station-configuration** command is used in the case of certain MMS over HTTP requests without the User-Agent header in the request.
- CSCdz62856

Transaction logs exported from Content Engines to remote servers using File Transfer Protocol (FTP) are shown to be truncated on those remote servers when network connectivity is slow.
- CSCdz63262

Exiting a Telnet session while running the **show tech-support** command causes high processor usage.

- CSCdz63382
Although multiple bit rate (MBR) files can be played as video on demand (VOD) files using Windows Media Player 9, doing a fast forward or rewind of the MBR files causes the “An attempt was made to seek or position past the end of a buffer” message to be displayed and the connection to be terminated. This symptom is observed only with MMS UDP (MMSU) protocol and not with MMS TCP (MMST) and Windows Media Technologies (WMT) HTTP protocols.
- CSCdz65241
The Content Engine does not validate content requests if an outgoing proxy server is configured. Therefore, it will forward even junk requests to the outgoing proxy server.
- CSCdz66346
A core dump is generated when the header returned by the MMS server is not appropriate.
- CSCdz69545
Content Engines and Content Routers do not support requests without host names. All HTTPS requests from clients are encrypted and do not contain host names. Therefore, all Remote Procedure Call (RPC) traffic over Secure Socket Layer (SSL) is rejected by the Content Engine or Content Router.
- CSCdz70756
Windows Media Player 7.01 buffers a live stream while playing it, either at the beginning or in the middle of the stream.
- CSCdz72294
An appropriate error message is not displayed when an attempt is made to start or stop a nonexistent multicast station using the **wmt multicast-station {start name | stop name}** command.
- CSCdz74540
Certain operations, such as deletion of files, fail to work on the Microsoft SharePoint server. These operations involve the use of WebDAV (Web-Based Distributed Authoring and Versioning) methods, which cause the Microsoft SharePoint server to return a “207 Multi-Status” response to the Content Engine and terminate the connection.
- CSCdz86277
Local users cannot be added to or deleted from the Content Engine. Also, remote user authentication fails because the snmpd.log file occupies a large amount of disk space in the temp directory.
- CSCdz88575
On a CE-590 running ACNS software, Release 4.2.3 using Web Cache Communication Protocol (WCCP), wireless clients connecting through the Ethernet ports 1/1 through 1/5 are unable to access the Internet, resulting in a processor usage of 100 percent.
- CSCdz90333
In certain specific cases, the cache process crashes when the DNS lookup fails and an attempt is made to insert a host name into the error message.
- CSCin25198
In the Content Engine Graphical User Interface (GUI), the Back button on the WMT multicast page works properly until you click the Help button. When you click the Help button, a loop is formed between the WMT Multicast page and the Help page, making it impossible to access other pages.

- CSCin29973
In the Content Engine GUI, no option is available on the TACACS page to enable or disable TACACS authentication.
- CSCin33106
Support for exporting the Real-Time Streaming Protocol (RTSP) transaction log is not provided in ACNS software, Release 4.x.
- CSCin33885
E-CDN application contents are not served in response to requests from clients if Internet Cache Protocol (ICP) client functionality is enabled. This symptom occurs when the Content Engine acting as an ICP client is configured with an ICP server as a parent and to fetch cache miss from the child Content Engine.

Documentation Updates

This section describes some documentation updates.

SmartFilter and the No-Auth Rule Interaction

The **no-auth** rule permits specific login and content requests to bypass authentication and authorization features such as LDAP, RADIUS, SSH, or TACACS+. For example, any requests from the source IP address (src-ip) of 172.16.53.88 are not authenticated.

```
ContentEngine(config)# rule enable
ContentEngine(config)# rule action no-auth pattern-list 1 protocol all
ContentEngine(config)# rule pattern-list 1 src-ip 172.16.53.88 255.255.255.255
```

If ACNS software is configured for authentication and SmartFilter URL filtering, requests that are allowed to bypass authentication will also bypass the URL filter.

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*

Software Documentation

- *Cisco ACNS Software Caching Configuration Guide, Release 4.2*
- *Cisco ACNS Software Command Reference, Release 4.2*
- *Cisco ACNS Software E-CDN Administrator's Guide, Release 4.2*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *Release Notes for Cisco ACNS Software, Release 4.2*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.0.2*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this 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 may have 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.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) 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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- 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

To obtain customized information and service, you can self-register on Cisco.com at this 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 levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- 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.

Cisco TAC Website

You can use the Cisco TAC website 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 website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require 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 this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this 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). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:
http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:
http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.



Copyright © 2003 Cisco Systems, Inc. All rights reserved.