



# Release Notes for Cisco ACNS Software, Release 4.2.9

---

April 28, 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 4.2.9. These release notes describe the following topics:

- [Contents, page 1](#)
- [New and Changed Information, page 2](#)
- [Additional Hardware Supported, page 3](#)
- [Caveats, page 4](#)
- [Documentation Updates, page 9](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, page 10](#)
- [Obtaining Technical Assistance, page 12](#)
- [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 4.2.9.

## New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 4.2.9

The ASCII password support for TACACS+ authentication feature is new.

### Support for an ASCII Password During TACACS+ Authentication

TACACS+ is an authentication method that validates all users on an individual basis before they can gain access to a Content Engine. A new global configuration command, **tacacs password ascii**, has been added in ACNS software, Release 4.2.9. This command can be used to specify the TACACS+ password type as ASCII. The default password type is PAP (Password Authentication Protocol). In releases prior to ACNS software 4.2.9, the password type is not configurable. When users need to login to a Content Engine, a TACACS+ client sends the password information in PAP format to a TACACS+ server. However, TACACS+ servers that are configured for router management require the passwords to be in ASCII clear text format instead of PAP format to authenticate users logging into the Content Engine. Therefore, in ACNS software, Release 4.2.9, the password type to authenticate user information has been made configurable from the CLI. An example of the **tacacs password ascii** command together with the **no** version of the command and **show tacacs** commands are show below:

```
ContentEngine(config)# tacacs password ?
  ascii  Utilize ASCII password type for authentication (PAP is default)
ContentEngine(config)# tacacs password ascii
ContentEngine# show tacacs
  Login Authentication for Console/Telnet Session: enabled (primary)
  Configuration Authentication for Console/Telnet Session: enabled (primary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key           = *****
Timeout       = 5
Retransmit    = 2
Password type: ascii

Server                               Status
-----
172.19.226.182                        primary
```

```

ContentEngine(config)# no tacacs password ascii
ContentEngine# show tacacs
  Login Authentication for Console/Telnet Session: enabled (primary)
  Configuration Authentication for Console/Telnet Session: enabled (primary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: pap

Server                               Status
-----
172.19.226.182                        primary

```

**Note**

When the **no tacacs password ascii** command is used to disable ASCII password type, the password type is once again reset to PAP.

The TACACS+ client can send different requests to the server for user authentication. The client can send a TACACS+ request with the Password Authentication Protocol (PAP) authentication type. In this scenario, the authentication packet includes both the username and the user's password. The server must have an appropriately configured user's account. Also, the client can send a TACACS+ request with the ASCII authentication type as another option. In this scenario, the authentication packet includes the username only and waits for the server response. Once the server confirms that the user's account exists, the client sends another Continue request with the user's password. The authentication server must have an appropriately configured user's account to support either type of password.

## Additional Hardware Supported

ACNS software, Release 4.2.9 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
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 ACNS software, Release 4.2.9, and caveats that were resolved in this release. Caveats describe unexpected behavior in ACNS software, Release 4.2.9. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Open Caveats - ACNS Software, Release 4.2.9

- 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.
- CSCdy68833  
Symptom: A core dump is seen under /local1/core\_dir for Real-Time Streaming Protocol (RTSP) 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.
- 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.
- 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.
- CSCeb09185  
Symptom: The following message appears during bootup or when **disk** commands are used:  
`You are using unsupported hardware.`  
Condition: This occurs on a CE-560, CE-590, and CE-7320 with Storage Arrays, SA-7 and SA-14 and running ACNS software, Release 5.0.3 or earlier.  
Workaround: Ignore the warning message. The storage array actually works, although the warning message informs that it is not working.
- 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 4.2.9

- CSCdy16548  
When you use ACNS software to verify Windows NT LAN Manager (NTLM)-supplied passwords on a Windows 2000 server or Windows XP system, if the password is longer than 14 characters, the authentication fails.
- CSCdy35116  
The syslog file is not created after it is manually deleted, and system logging is not restarted until you reconfigure the ACNS software using the **logging disk filename filename** CLI command.
- CSCdz10104  
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 but then stops. This problem is observed when the content items or files do not have filename extensions (for example, the filename is "123" instead of "123.gif").
- CSCdz50695  
When a Content Engine receives a "100 Continue" response after a POST request, it switches itself to 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 (meant for other servers) from the client and instead passes them directly to the same 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.

- CSCdz51974

When a web server tries to authorize requests from different Content Engines in a cache farm for Java class objects and related GUI files for the Java monitor (for the purpose of viewing the statistics from all Content Engines in a cache farm), certain Internet Explorer (IE) browser versions record an error in handling 401 (Unauthorized Exception) responses from the web server for Java applets. In contrast, in Netscape browsers, an authorization dialog box is displayed automatically for each and every Content Engine in the cache farm. This process of logging in to each Content Engine needs to be done manually in IE, which is cumbersome when there are a large number of Content Engines in the cache farm.

- CSCdz53969

When you reboot the Content Engine, the Cache application crashes because of memory corruption in the initialization phase. This problem has been observed on the CE-7320 only.

- CSCdz56234

The **ip domain-name** CLI command cannot be used to specify more than one domain. 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.

- CSCdz61110

When the Windows Media Technologies (WMT) server is disabled on a Content Engine, the WMT content served by a standard HTTP server is not preloaded.

- CSCdz68835

A Content Engine under heavy load might generate a crash file when an attempt is made to remove a cached object twice.

- CSCdz70582

A “The page cannot be displayed” error message occurs when a web page takes about 5 to 8 minutes to download after background processing of queries. This error occurs because the cache does not support Hypertext Transport Protocol Secure (HTTPS) keepalive messages. For HTTPS connections, the default timeout value is 5 minutes. When no keepalive messages are sent by the Content Engine to the clients and to the edge Content Engines, the connection is closed.




---

**Note** In ACNS software, Release 4.2.9, you can force the Content Engine to send keepalive probes using the **https tcp-rw-timeout** global configuration command. When the HTTPS TCP keepalive feature is enabled, the Content Engine sends TCP keepalives on idle TCP connections using keepalive configuration parameters such as TCP keepalive timeout, TCP keepalive probe count, and TCP keepalive probe interval. The **https tcp-rw-timeout** command allows you to configure a maximum read/write timeout of 3600 seconds; that is, HTTPS keepalives are sent for the specified period.

---

- CSCdz74690

The IP address on an interface can be accessed even though the interface has been disconnected. This problem occurs only if all the following conditions are met:

- The Content Engine has one physical interface connected to the router’s VLAN X and has a valid IP address configuration A.x in IP subnet A.0.
- The Content Engine’s other interface is not connected. However, it has an IP address B.x from a different subnet B.0.
- IP subnet B.0 is also configured over VLAN X on the router side. At this time, the router can access IP address B.x through the connected interface.

- CSCea17342  
The Packets Sent and Packets Received parameters shown in the output of the **show interface** command are incorrect. These parameters stop incrementing after reaching a certain specific value.
- CSCea20850  
The Cache application might crash because of error conditions while handling disk input/output.
- CSCea22087  
A CE-7320 running ACNS software, Release 4.2.5 stops and enters the kernel debugger (KDB) mode. This problem occurs when the CE-7320 is running WCCP Version 2 with the IP spoofing feature enabled.
- CSCea32949  
NTLM authentication fails when accented characters are used to specify clear-text passwords in the Netscape browser. The LAN Manager encryption incorrectly encrypts the accented characters, because it recognizes only ASCII characters.
- CSCea38131  
A Content Distribution Manager running ACNS software, Release 4.x can be used as an HTTP proxy by users who are able to connect to the Content Distribution Manager, thereby enabling unauthorized access. This problem occurs because there is no option to turn off the incoming HTTP proxy functionality of the Content Distribution Manager.
- CSCea40434  
The Cache application stops unexpectedly and generates core files during file system operation when the **rule action cache** global configuration command is used to override HTTP response headers while caching objects and some servers return strange responses (without headers).
- CSCea43384  
When clients use long-persistent connections with the Content Engine as a reverse proxy server, the Content Engine appears to be leaking packets received from port 8999. This results in the remote host receiving a packet from port 8999 and sending a reset (RST) bit, causing the termination of the connection.
- CSCea49561  
Chunked HTTP request packets fail to pass through the Content Engine. Although the first packet of the request reaches the Content Engine, subsequent requests do not, causing the server to return a 500 (Internal Server Error) message to the client. This problem occurs only with chunked HTTP request packets.
- CSCea49975  
Multicast distribution is not reinitialized whenever there is an IP address change and WCCP Version 2 is running on a Content Engine Network Module. When this problem occurs, the WCCP redirection services on the Content Engine are disabled, and none of the routers running WCCP Version 2 are able to see this Content Engine.
- CSCea50090  
The **find-pattern** EXEC command, used to search for a particular pattern in a file, does not return the desired output when multiple spaces are used in the regular expression to be matched (the search string) and are enclosed within quotes.

- CSCea50102  
When the number of characters in the search expression to be matched is greater than 19 and the characters are enclosed within quotes, the **find-pattern EXEC** command, used to search for a particular pattern in the file, does not return the desired output.
- CSCea53039  
The Content Engine stops abruptly and generates a core file after the action to override the HTTP response headers and cache the pattern list “?” is enabled using the following command:  

```
rule action cache ttl hours 2 .\?*
```
- CSCea53067  
The WCCP flow table displaying the standard web caching service packet flows is found to be incorrect after the Cache application restarts automatically. However, because the view of the WCCP router seeing the Content Engine does not change, WCCP assumes that it is not necessary to update the standard web caching service packet flows.
- CSCea53748  
The CE-7305 enters KDB mode while attempting to remove an IP address from a PortChannel interface.
- CSCea55091  
Playing certain Windows Media Audio (.wma) files causes the Microsoft Media Server (MMS) to restart automatically.
- CSCin27564  
Unwanted messages are displayed when the user configures group name-based access control lists.
- CSCin33541  
The SNMP agent does not generate the entConfigChange trap on a Content Engine Network Module running ACNS software, Release 4.2.6.
- CSCin34010  
When the Content Engine receives an HTTP request from a client using a method that is not in the list of supported methods, the ACNS software does not add the method to the list of unsupported methods and return an appropriate error description to the client.
- CSCin35167  
When RealSubscriber is enabled using the **real-subscriber enable** global configuration command, an improper error message is displayed.
- CSCin35224  
The **http add-method** global configuration command allows a method name, consisting of two words separated by a space and enclosed within double quotes, to be specified.
- CSCin35520  
A WCCP Version 1 core dump is generated during bootup of a Content Engine Network Module running ACNS software, Release 4.2.7.
- CSCin35737  
An option to enable the RADIUS database for user authentication is not available in the Authentication Configuration window on the Content Distribution Manager GUI.

- CSCin35846  
A core file is generated by WCCP Version 1 when an IP address is not configured on the Content Engine network interface. WCCP Version 2 requires that the Content Engine be restarted if an IP address is configured after WCCP is enabled.
- CSCin36770  
When the Content Engine is unable to authenticate the user using the TACACS+ primary authentication database, it fails to query the secondary authentication database.
- CSCea48537  
The Cache application crashes while it is configuring bandwidth for an interface.
- CSCea61874  
When there are two concurrent requests for the same disk object, the Cache application restarts unexpectedly. This problem occurs when the load on the Content Engine is high and the size of the objects is greater than 512 KB.
- CSCea63278  
When a request from a client to a WMT server is specified with a double space between the host name and the relative URL, the WMT server infinitely loops back on itself. This problem causes the utilization of all resources available on the Content Engine, thereby slowing down other processes running on the Content Engine.
- CSCea65822  
Content Engine bypass does not work when IP spoofing is enabled with Layer 2 redirect. In this case, the packets sent back by the origin server to the client are not sent by the Content Engine to the router. Instead, these packets are sent to the IP layer and are dropped. Also, the bypass entries are displayed in the output of the **show bypass list** command.
- CSCin35743  
An error message is displayed in the Cache on Abort window on the Content Engine GUI when valid values are configured for maximum and minimum threshold.

## 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 websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](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 regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order monthly or quarterly subscriptions 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](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>
- 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](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) 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://tools.cisco.com/RPF/register/register.do>

## 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: the Cisco TAC website and the Cisco TAC Escalation Center. The type 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. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

## Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. 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/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation 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 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](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 quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating 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](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

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