



Release Note for Cisco ACNS Software, Release 5.4.7

November 5, 2007



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.

Contents

This release note document contains information about the Cisco Application and Content Networking System (ACNS) 5.4.7 software. This document describes the supported hardware, and the open and resolved caveats for software version 5.4.7. The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media.

This release note describes the following topics:

- [Hardware Platforms Supported in ACNS Software](#)
- [Software Component Versions Supported in ACNS Software](#)
- [Operating Considerations](#)
- [Software Version 5.4.7 Open Caveats](#)
- [Software Version 5.4.7 Resolved Caveats](#)
- [Related Documentation](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

Hardware Platforms Supported in ACNS Software

The ACNS software runs on Cisco Content Engine, Content Distribution Manager, Content Router, and Wide Area Application Engine (WAE) hardware platforms. The ACNS 5.4.3 release is the required minimum software release for the WAE-512 and WAE-612 appliances. The ACNS 5.3.3 release is the required minimum software release for the WAE-511, WAE-611, and WAE-7326 appliances.

Table 1 shows the hardware platforms and the minimum ACNS software release in which each is supported.

Table 1 Hardware and ACNS Software Compatibility Matrix

Hardware Model	ACNS Software Support				
	5.3.1	5.3.3, 5.3.7	5.4.1	5.4.3, 5.4.5, 5.4.7	5.5.x
CE-507 CE-560 CE-590 CR-4430 CDM-4630	X	X	X	X	X
CE-7320 CDM-4650	X	X	X	X	X
NM-CE-BP-SCSI NM-CE-BP-40G NM-CE-BP-80G	X	X	X	X	X
CE-510 CE-510A CE-565 CE-565A	X	X	X	X	X
CE-7305 CE-7305A CE-7325 CE-7325A	X	X	X	X	X
CE-511 CE-566	X	X	X	X	X
WAE-511 WAE-611		X	X	X	X
WAE-7326		X	X	X	X
WAE-512 WAE-612				X	X

Software Component Versions Supported in ACNS Software

Table 2 describes which SmartFilter and Websense versions are supported in the ACNS software releases.

Table 2 *Component Versions Supported in ACNS Software Releases*

ACNS Software Release	SmartFilter Version Supported	Websense Version Supported
ACNS 5.2.1	Version 4.0.1	Version 5.2
ACNS 5.3.x	Version 4.0.1	Version 5.2
ACNS 5.4.1	Version 4.0.1	Version 5.5.2 ¹
ACNS 5.4.x	Version 4.1.1	Version 5.5.2
ACNS 5.5.x	Version 4.0.1	Version 5.5.2

1. The integrated Websense Enterprise software Version 5.5 in the ACNS 5.4 software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM. When additional Websense components are enabled (such as the Network Agent), ACNS software requires a minimum of 1 GB of RAM.

Performance is optimal when Websense Enterprise Manager, the Websense Policy Server, and all other Websense components are situated in the same LAN. If all components are not in the same LAN, you might experience communication latency between Websense Enterprise Manager and other components. A significant increase in latency can lead to a communication failure.

Operating Considerations

The following operating considerations apply to the ACNS 5.4.x software. It includes the following sections:

- [Multicast-In Sources in SSPLs Not Supported for Windows Media Streaming](#)
- [No Downgrade Script to ACNS Releases Later than 5.3.3](#)
- [RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software](#)
- [Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software](#)
- [Media File System Issues When Downgrading to ACNS 5.0 Software](#)
- [SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release](#)
- [Interoperability with ICAP Vendors](#)
- [ICAP Performance](#)
- [ICAP Maximum File Size Supported](#)
- [Matrix of Supported Caching, Filtering, and Authentication Methods](#)

Multicast-In Sources in SSPLs Not Supported for Windows Media Streaming

Multicast-in source objects in server-side playlists are not supported for Windows Media streaming. If you have such an unsupported configuration, the Windows Media stream will fail, and the problem will be identified in the syslog file, as shown in the following example:

```
Jul 9 21:30:09 new-stream-ce2-158-3 mms_server: %CE-WMT-2-512078: Multicast-in with SSPL
source is not supported
```

No Downgrade Script to ACNS Releases Later than 5.3.3

There is no downgrade script in the ACNS 5.4 code base to downgrade directly to ACNS 5.3.x releases that are later than ACNS 5.3.3. To downgrade from ACNS 5.4 software to ACNS 5.3.x software you must use the following guidelines:

- Use the Downgrade5_4_to_5_3_3 downgrade script if you are downgrading from ACNS 5.4 to any ACNS 5.3 version that is greater than or equal to ACNS 5.3.3.
- Use the Downgrade5_4_to_5_3 downgrade script if you are downgrading from ACNS 5.4 to any ACNS 5.3 version that is earlier than ACNS 5.3.3.
- Before or after you run the downgrade script, you must install the version of ACNS 5.3.x software that you need.

RAM Requirements for ACNS 5.4 Software and Websense 5.5 Software

The integrated Websense Enterprise software Version 5.5 in the ACNS 5.4 software requires a minimum of 512 MB of RAM. We recommend that you upgrade the RAM on your device to 512 MB or greater, or move your integrated Websense server to another device that has at least 512 MB of RAM.

Websense Issues When Downgrading to the ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to either ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. The ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed. However, in the ACNS 5.3.1 software and later releases, the following error message is displayed to notify you about this Websense downgrade issue:

```
WARNING:
Websense does not support downgrade
Hence removing /local/local1/WebsenseEnterprise
Websense will stop working after copy ftp install
```

To avoid this problem when downgrading from the ACNS 5.3.x or ACNS 5.2.x software to either ACNS 5.1.x software or ACNS 5.0.x software, follow these steps:

-
- Step 1** Disable the local (internal) Websense server on the Content Engine.
 - Step 2** Deactivate the Websense services on the Content Engine.
 - Step 3** Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.
-

Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with the ACNS 5.1 software and later releases, and then downgrade to the ACNS 5.0 software, the mediafs disk space assignment is lost and reverts to the ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in the ACNS 5.1 software. Because the ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to the ACNS 5.0 software, use the CLI (**disk config EXEC** command) or the GUI to assign the mediafs disk space.

Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

SmartFilter Issues When Upgrading or Downgrading to Another ACNS Software Release

When you upgrade or downgrade the Content Engine to a different release of the ACNS software, if there is a difference in the SmartFilter plug-in version, the SmartFilter database and configuration files are deleted and default configurations are loaded. This change occurs because the configuration details might be changed with each new version of SmartFilter software. After each upgrade or downgrade of the SmartFilter plug-in, a fresh database has to be downloaded from the SmartFilter Administration Console to the Content Engine. (For a description of which SmartFilter versions are supported in the ACNS software releases, see [Table 2](#).)

Interoperability with ICAP Vendors

The Internet Content Adaptation Protocol (ICAP) is an open standards protocol for content adaptation, used typically at the network edge. Content adaptation includes virus scanning, content translation, content filtering, content insertion, and other methods of improving the value of content to end users. ICAP specifies how a Content Engine, acting as an HTTP proxy server, can communicate with an external device that is acting as an ICAP server to filter and adapt the requested content.

ICAP provides two content-processing modes for HTTP services. These modes define the transactions that can occur between a Content Engine acting as an ICAP client and an ICAP server. The two modes are as follows:

- Request modification (reqmod)—Allows modification of requests as they are sent from the Content Engine to the ICAP server on their way to the origin server. The ICAP server can modify these requests depending on the services requested.
- Response modification (respmo)—Allows modification of requests after they return from the origin server. The ICAP server only acts on requested objects after they return from the origin server.

The following is a complete list of the ICAP vendors that have been certified to interoperate with the Content Engine:

- TrendMicro for reqmod and respmod
- Symantec for respmod

ICAP Performance

With the respmod vectoring point, which is used by virus-scanning ICAP vendors, the performance of the Content Engine model CE-7305 will be 300 transactions per second.

With the reqmod-precache vectoring point, which is used by URL filtering ICAP vendors, the performance of the Content Engine model CE-7305 will drop 20 percent from the rated performance.

The performance of the Content Engine will be limited by the performance of the ICAP server.

ICAP Maximum File Size Supported

For ACNS 5.4.x software and later, the maximum file size that is supported in the ACNS software is 2 GB. Files that exceed this size limit are not supported for ICAP processing.

Matrix of Supported Caching, Filtering, and Authentication Methods

Table 3 lists the caching, filtering, and authentication methods supported by Content Engines that are running the ACNS 5.4.x software. An asterisk (*) indicates that a feature is supported for that particular protocol.

Table 3 Caching, Filtering, and Authentication Methods and Related Protocol Support

Protocol	Filtering				Proxy Authentication			
	Caching	N2H2	Websense	SmartFilter	RADIUS	LDAP	NTLM	TACACS+
HTTP	*	*	*	*	*	*	*	*
FTP-over-HTTP	*	*	*	*	*	*	*	*
HTTPS-over-HTTP	*	*	*	*	*	*	*	*
RTSPG	*							
MMSU	*							
MMST	*							
MMS-over-HTTP	*				*	*		
HTTP-WCCP	*		*	*	*	*	*	*
FTP-WCCP (native FTP)	*							
HTTPS-WCCP	*		*	*				
RTSPG-WCCP	*							
MMSU-WCCP	*							
MMST-WCCP	*							
MMS-over-HTTP -WCCP	*				*	*		

Software Version 5.4.7 Open Caveats

This section lists the open caveats in the ACNS 5.4.7 software release.

- **CSCsd68185**—An error condition may be entered by the CE causing the authmod process to generate a core file when the number of TPS is 100 or greater, and NTLM authentication is enabled. Workaround: None.
- **CSCsj07986**—Core dump may occur on the ACNS while querying `cceWmtTotalClientErrors`. Workaround: None. The SNMP process is restarted automatically.
- **CSCsj58290**—WMP display one of the following error messages when you attempt to view specific WMV files using the ACNS WMT server:
 - When using WMP version 10—*Windows Media Player encountered an unknown error*. This may occur when another program or operating system component encounters a problem, but does not communicate the nature of the problem to the Player.
 - When using WMP version 9—*Windows Media Player encountered an unknown error*. The occurs when WMP is set to use only TCP and is applicable for RTSP protocol, which may be also used for `mms://` kind of URLs.

Workarounds: Set WMP to use only the UDP option (which may not work due to FW/NAT issues) or use a later version of ACNS, such as 5.5.7.

- **CSCsj82298**—When you make a change to an item in a device group, the complete configuration configured in that device group is pushed to all devices in the group. This includes the WCCP redirection/return selections. Within these is the I2-return line. When the content engine gets this line it pushes this to the router. The router sees the I2-return line and notifies the cache that it does not support a I2-return line. At the same time, it renegotiates the WCCP parameters. This causes the Catalyst 6500 series switch to drop the current WCCP session. Workaround: If this issue occurs when you try to modify the bypass list, create a new device group call `BypassListEntriesDeviceGroup` and add all required content engines to this group. In this new device group only bypass entries are configured and these will be the only configuration pushed during the operation.
- **CSCsk02280**—Messages similar to HTTP proxy down are logged in the syslog. The issue occurs when the cache or RTSP process is overloaded. Workaround: None.
- **CSCsk02350**—WCCP redirected request fails when a proxy set in the player is set in the QT player in a WCCP redirection scenario. Workaround: None.
- **CSCsk22084**—The alarm lingers in the GUI even when the CLI show alarms on the CE are blank. When the critical alarms has been fixed, the corresponding alarm is cleared in the CE, but not in CDM GUI. Workaround: On the CDM, use the **no cms enable** command and then issue the **cms enable** command.
- **CSCsk50224**—Rule action rewrite is not working for mms protocol when you enable rule action rewrite for a server IP address with another server IP address. The scenario occurs only for mmsu and mmst requests. Workaround: None.
- **CSCsk63735**—CPU usage may be high to 100% on the CE even if no tasks are running on it. The DNS process recovers from intermittent connection failures between the DNS process and the DNS server configured on the CE. Workaround: Restarting the DNS process may resolve this issue.
- **CSCsk93119**—You may receive multiple authentication prompts while using NTLM as an authentication mechanism. The issue occurs only when the ACNS WAE is configured for an ISA server as an outgoing proxy and when NTLM authentication is enabled in the ISA Server. This issue may not occur for all requests. This issue may not occur when the ACNS WAE is configured as an outgoing proxy. Workaround: None.

Software Version 5.4.7 Resolved Caveats

This section lists the caveats that have been resolved in the ACNS 5.4.7 software release.

- **CSCsc10623**—When you issue the **sh http-authcache** command, the domain name is displayed in lowercase.
- **CSCsd91271**—Requests are rejected when the device attempts to contact the outgoing proxy at port 65533. This occurs when the outgoing proxy goes down and a request is received from the origin server.
- **CSCse04951**—Customer applications may fail intermittently through a CE when the client stations receive frames with incorrect TCP checksums. When an application makes an HTTP or FTP-over-HTTP request for data, the data is non-cacheable and arrives from server in IP fragments.
- **CSCsg60334**—An IP address configured on CE interface is also announced to the WCCP router if the interface is administratively shut down. This issue occurs with routers affected by CSCee02118 because they fail to perform WCCP redirection entirely or blackhole the traffic.
- **CSCsg62343**—Program details are not displayed when you issue the **sh prog** command using a program name as an attribute.
- **CSCsg97879**—The Content Engine may generate a core file from the data server process.
- **CSCsh05777**—No audio is available when playing a live event using msoftlive meeting and using cache as a proxy.
- **CSCsh07157**—Under rare conditions with an RTSP streaming server configured, the RTSP DSS process may generate a core file during a content engine image upgrade process.
- **CSCsh43705**—When a leading cache engine is removed from a cache farm, the remaining CE drops all assigned wccp masks and then starts adding them one by one. When the removed CE returns, mask assignments are restored inconsistently, with masks moving between caches.
- **CSCsh63113**—A core file in the UniReceiver is generated approximately every hour when acquisition is enabled.
- **CSCsh69267**—The cache engine may stop responding.
- **CSCsi00029**—When you issue the **cache reset** command from exec mode, it does not reset the cache, and displays the following error message:


```
Cache Clear command is still pending, please retry later. (Error 1057).
perf-512-112#cache reset.
Cache Clear command is still pending, please retry later. (Error 1057)
```
- **CSCsi08998**—When SmartFilter is enabled, a message is written to the syslog for every blocked HTTPS Proxy connection, which blocks HTTPS proxy requests.
- **CSCsi16813**—When a client receives block pages for FTP-over-HTTP requests and ICAP and urlfilter are both enabled, the urlfilter blocks requests from 127.0.0.1.
- **CSCsi18571**—Replication CEs display inaccurate counts of channel contents as compared to root. The content mismatch occurs after a large amount of content is removed at the same time (for example, >10000) from the origin server for the channel.
- **CSCsi35189**—The total number of buckets assigned are assigned one at a time for a lead CE. For all the buckets to be assigned, it takes approximately 30 minutes. If there are more than two CEs, then one bucket at a time is assigned only to the lead CE. There is no impact to the other CEs in the web-cache farm.
- **CSCsi40391**—META REFRESH content is improperly formatted for dynamic bypass triggers from the CE.

- **CSCsi43638**—Configuration proxy-protocols outgoing-proxy exclude list [pattern] may match unexpected patterns in specific situations. The pattern contains only numbers, dot (.) and asterisk (*) characters. All domain names with the same initial numbers are also matched.
- **CSCsi43641**—An HTTPS proxy request is replied with "200 Connection established" when the destination IP address is unreachable.
- **CSCsi44425**—Packets redirected to a CE counter are incremented when I2-redirection is enabled.
- **CSCsi45941**—The NSC file that is delivered contains the loopback IP address of a non-location leader, which breaks the multicast and unicast deliveries if it is directed to a non- location leader Content Engine for a live multicast program.
- **CSCsi47104**—The cache process gets into a loop, and the output of the **top** command shows the cache process using 99.9% of the CPU time.
- **CSCsi47286**—When SmartFilter is enabled, a cache core file is generated in /local1/core_dir. The core file is in sf_lookup_ldap_groups.
- **CSCsi57705**—When using the user service in websense and the user name contains space, users cannot be identified. This condition breaks URL filtering.
- **CSCsi60502**—When you issue the **show memory** command, the application memory usage output of various modules is not displayed. Only the column headers are displayed.
- **CSCsi71104**—The **find** command wildcard options do not work.
- **CSCsi75165**—When append x-forward is configured, the device incorrectly appends the IP address of 127.0.0.1 as the IP address
- **CSCsi83884**—FTP-export generates a core dump when you specify an invalid path for an SFTP server.
- **CSCsi85829**—A dual CPU device displays 100% when operating for long durations (such as greater than 40 weeks) under a minimum load.
- **CSCsi87691**—When the device receives a request for a prepositioned file and TTL is configured, an error message reports that there is not enough bandwidth.
- **CSCsi88884**—When slowstart is enabled, the assignment is masked.
- **CSCsi97636**—The cache process stop functioning when the request header size exceeds 16K.
- **CSCsj10769**—FTP_export stops functioning when SFTP export is configured to a correct location for exporting log files.
- **CSCsj14495**—The DNS process may generate a core file if a content engine is unable to reach a DNS server for an extended period of time. The network unreachable condition that leads to this core file may be seen by the following messages in the content engines syslog file:

```
Tue Jun  5 08:01:24 2007: sendto: Network is unreachable
```
- **CSCsj19799**—HTTPS requests from clients are not forwarded to the outgoing proxy. Instead, the clients receive the following error page: " All configured outgoing proxies have failed to server request. Please contact administrator to check outgoing proxy or configuration."
 During the failure, the content engine continues to send monitor keepalives to the outgoing proxy server, and the replies are received correctly.
- **CSCsj26798**—An SNMP core occurs in the CE when querying for ACTONA-ACTASTOR-MIB (which is not supported in ACNS) for the first time.
- **CSCsj36452**—SmartFilter may not work on certain web sites when the device is running for an extended period (for example, up to two weeks).

- **CSCsj47345**—The CE seems to fetch content from the origin server even when the content is not stale. This occurs when there is a must-revalidate header without a last modified header.
- **CSCsj49720**—When deleting a reference to a pac file template, the other previously configured pac template reference stops functioning.
- **CSCsj52850**—When bypass auth-traffic and ICAP service are both configured and enabled on the ACNS, authentication requests are not bypassed.
- **CSCsj53163**—When error-handling a reset or when a send-cache error is configured, bypass authentication traffic is enabled.
- **CSCsj64516**—The CE does not forward cookie-related information from the client to a server for MMS-over-HTTP requests.
- **CSCsj66588**—A 406 response code is generated when the proxy.pac is requested and proxy-auto-config is disabled and the request is destined for another server.
- **CSCsj98779**—An McastSender or McastReceiver core may occur in the CE preventing multicast distribution progress if the port channel is configured on the CE and the CE is multicast enabled and assigned to a multicast channel and cloud.
- **CSCsk02645**—When DNS is configured for round-robin, requests for a broadcast alias are redirected to an incorrect proxy instead of to the origin server.
- **CSCsk06669**—When a CE is configured with websense and ICAP, and both ICAP modes are enabled, the icap_daemon may stop functioning. This condition prevents the CE from serving the HTTP requests for approximately 30 seconds until the icap_daemon restarts.
- **CSCsk20769**—The software was updated to accommodate the change in New Zealand daylight savings times and dates.
- **CSCsk42566**—Playback fails for URL rtspu://10.77.157.189/100kbs.wmv?a=b&http://asfasfa. The presence of // in the URL is blocking playback for RTSP.
- **CSCsk50003**—A core file is generated in a CE when a multicast device is configured and you issue the **sh programs program name <multicast station name>** command.
- **CSCsk55302**—The SNMP process stops functioning when the device is booting up.
- **CSCsk92804**—LDAP group searches may result in improperly populated group membership lists for users whose primary group is Domain Users. Users may be able to access resources, even if access-lists specifically deny access to those resources, based on improperly cached credentials.
- **CSCsl16108**—Ftp-native proxy authentication requests are not authenticated properly. This occurs only when the CE is configured for ftp-native proxy with ntlm authentication and access-list configured. HTTP requests are authenticated properly.

Related Documentation

The ACNS documentation set includes the following:

- [Hardware Documentation](#)
- [Software Documentation](#)
- [Online Help](#)

Hardware Documentation

ACNS documentation includes the following hardware guides:

- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *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*
- *Cisco Regulatory Compliance and Safety Information for the Content Networking Product Series*

Software Documentation

ACNS documentation includes the following software guides:

- *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.4*
- *Cisco ACNS Software Command Reference, Release 5.4*
- *Cisco ACNS Software API Guide, Release 5.4*
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.4*
- *Release Notes for Cisco ACNS Software Program Manager for IP/TV, Release 5.4*

Online Help

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button. ACNS software includes the following online help systems:

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0612R)

