



Release Notes for Cisco Unified Service Monitor 2.1

Revised: April 22, 2009

Cisco Unified Service Monitor is a product from the Cisco Unified Communications Management Suite. These release notes provide:

- [New Features, page 1](#)
- [Product Documentation, page 2](#)
- [Related Documentation, page 2](#)
- [Supported Versions of Cisco Unified Communications Manager, page 3](#)
- [Supported Cisco 1040 Binary Image Files, page 7](#)
- [Known and Resolved Problems, page 8](#)
- [Documentation Updates, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 15](#)

New Features

The following changes and enhancements are included in Service Monitor 2.1:

- Support for Cisco Unified Communications Manager (Unified Communications Manager) 7.0(1).
- Added Unified Communications Manager credential support to enable Windows only authentication with Unified Communications Manager 4.x.
- Updated binary image for Cisco 1040 Sensors—SvcMonAA2_42.img. To load the image onto sensors, see *Quick Start Guide for Cisco Unified Service Monitor 2.1*.
- Clickable IP address links in Cisco 1040 Sensor reports for launching an Operations Manager Device Detail page for a device (Unified Communications Manager or gateway) that is a speaker or a listener.
- See [Table 7 on page 13](#) for problems that are resolved in this release.



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

Product Documentation


Note

The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

Table 1 describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available
<i>Release Notes for Cisco Unified Service Monitor 2.1</i>	<ul style="list-style-type: none"> • Within the Documentation folder on the product CD-ROM • On Cisco.com at http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/release/SrvMonRN.html
<i>Quick Start Guide for Cisco Unified Service Monitor 2.1</i>	<ul style="list-style-type: none"> • Within the Documentation folder on the product CD-ROM • On Cisco.com at http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/quick/guide/SMqsg21.html
<i>User Guide for Cisco Unified Service Monitor</i>	<ul style="list-style-type: none"> • Within the Documentation folder on the product CD-ROM • On Cisco.com at http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/user/guide/UserGuideforCiscoUnifiedServiceMonitor21.html
Context-sensitive online help	Click the Help link in the upper-right hand corner of the window or the help button in any dialog box.

Related Documentation


Note

The originally published printed and electronic documentation was included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

Table 2 describes the additional documentation that is available.

Table 2 **Related Documentation**

Document Title	Available on Cisco.com at These URLs
<i>Quick Start Guide for Cisco 1040 Sensor</i>	http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/quick/guide/1040qs21.html
<i>Release Notes for Cisco Unified Operations Manager 2.1</i>	http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.1/release/notes/SrvMonRN.html

Table 2 **Related Documentation (continued)**

Document Title	Available on Cisco.com at These URLs
<i>Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor)</i>	http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html
<i>User Guide for Cisco Unified Operations Manager</i>	http://cisco.com/en/US/products/ps6535/products_user_guide_list.html
<i>Release Notes for CiscoWorks Common Services 3.0.5 (Includes CiscoView 6.1.5) on Windows</i>	http://cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0/release/notes/CWCS_RNW.html
<i>Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Windows</i>	http://cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/cs305igw_1.html
<i>User Guide for CiscoWorks Common Services 3.0.5</i>	http://cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/user/guide/cs305ug.html

Supported Versions of Cisco Unified Communications Manager

When properly configured, Service Monitor can report on voice activity from the versions of Unified Communications Manager listed in [Table 3](#).

Table 3 **Unified Communications Manager Support**

Unified Communications Manager Version	Information Available from this Version
3.3 4.0 4.1	<p>The following information is available for Service Monitor to include in reports:</p> <ul style="list-style-type: none"> • Cluster ID • Call endpoints • Time stamp (Reflects call disconnect time) • Call duration • Call termination cause • Codec • Milliseconds of jitter • Number of lost packets

Table 3 Unified Communications Manager Support

Unified Communications Manager Version	Information Available from this Version
4.2	In addition to the information provided by earlier versions, MOS is available for Service Monitor to use in determining whether a threshold has been violated and, if so, send a trap. Other data, such as concealment ratio and severely concealed seconds, is also available for inclusion on reports and in traps.
4.3	
5.0	
5.1	MOS is calculated using the Cisco Voice Transmission Quality (CVTQ) algorithm on specific phones. To make CVTQ data available, you need to:
6.0	
6.1	<ul style="list-style-type: none"> • Ensure that you have applied any required patches to Unified Communications Manager.
7.0(1)	<ul style="list-style-type: none"> • Use the specified models of Cisco Unified IP phones with the specified protocol and firmware; these phones must be registered with Unified Communications Manager 4.2, 4.3, 5.0, 5.1, 6.0, 6.1, or 7.0(1).
	For more information, see the following topics:
	<ul style="list-style-type: none"> • Required Unified Communications Manager Patches and Workarounds, page 4
	<ul style="list-style-type: none"> • Supported Cisco Unified IP Phone Models and Phone Protocols, page 6
	<ul style="list-style-type: none"> • Enabling CVTQ Data on Supported Cisco MGCP Voice Gateways, page 7

Required Unified Communications Manager Patches and Workarounds

Problems with CVTQ data can occur due to known problems with certain versions of Unified Communications Manager. [Table 4](#) documents these problems.

Table 4 **Circumstances that Can Affect CVTQ Data**

Description	Circumstances
<p>Service Monitor CVTQ reports do not show any calls in a Unified Communications Manager 5.0 cluster</p>	<p>If a space is included in the cluster ID, an error occurs in a component of Unified Communications Manager, and CDRs and CMRs are not pushed.</p> <p>Bug ID: CSCsd81400</p> <p>This problem has been fixed and verified in Unified Communications Manager 5.0(3.9911.35).</p> <p>Workaround: If you do not have the Unified Communications Manager 5.0(3.9911.35) image or later, do the following.</p> <ol style="list-style-type: none"> 1. Change the cluster ID to a name that doesn't include a space; from Unified CallManager Administration: <ol style="list-style-type: none"> a. Select System > Enterprise Parameters. The Enterprise Parameters Configuration page appears. b. Change the cluster ID. c. Click Update. 2. Repeat this step for each Unified Communications Manager: <ol style="list-style-type: none"> a. From Cisco Unified CallManager Serviceability select Tools > Control Center - Feature Services. b. Select the Unified Communications Manager server. c. Click the Restart button. 3. Remove old files from the Unified Communications Manager 5.0 server: <ol style="list-style-type: none"> a. Log in to the server. b. Go to the <code>/var/log/active/cm/cdr</code> directory. c. Remove all files that start with <code>cdr_old cluster name_</code> and <code>cmr_old cluster name_</code>.

Supported Cisco Unified IP Phone Models and Phone Protocols

The following Cisco Unified IP phone models support the CVTQ algorithm in SCCP and—in most cases—SIP mode if they have the 8.0(3) firmware which can be downloaded from Unified Communications Manager versions 4.2, 4.3, 5.x, 6.0, 6.1, and 7.0(1).


Note

For Cisco Unified IP phone models to support the CVTQ algorithm in SIP mode, you must enable Call Stats in the SIP profile. For more information, select the appropriate version of *Cisco Unified Communications Manager Administration Guide* at this URL:

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 5 Cisco Unified IP Phone Models that Support the CVTQ Algorithm

Model	Mode in Which CVTQ is Supported	
	SCCP	SIP
7906	X	X
7911	X	X
7921	X	X
7931	X	X
7940	X	—
7941	X	X
7942	X	X
7945	x	x
7960	X	—
7961	X	X
7962	X	X
7965	x	x
7970	X	X
7971	X	X
7975	x	x

No other Cisco Unified IP Phone models support CVTQ.


Note

The 8.0(3) phone firmware is also accessible from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>. (You must be a registered user of Cisco.com and log in to download the firmware.)

Enabling CVTQ Data on Supported Cisco MGCP Voice Gateways

To enable CVTQ data on Cisco MGCP voice gateways, you need the correct Cisco IOS software and DSP hardware and you must enable voice quality statistics on the voice gateway. Ensure that you have:

- Cisco IOS 12.4(4)T or later.
- TIC5510 DSP hardware—TIC5510 DSP supports the DSP/KF voice quality metric that Service Monitor needs. To confirm that a voice gateway has TIC5510 DSP, look for 5510 in the output of this command:

```
show voice dsp detailed
```

For more information, see *Cisco IOS Voice Command Reference* at this URL:

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html

The platforms on which TICDSP5510 is supported are:

- Cisco 2800 series and Cisco 3800 series integrated services routers with PVDM2 modules
- Cisco VG224 voice gateway
- Cisco IAD2430 series integrated access devices
- Cisco 2600XM, Cisco 2691, Cisco 3700 series access routers, Cisco 2811, Cisco 2821, Cisco 2851, and Cisco 3800 series integrated services routers with the following network modules:
 - NM-HDV2
 - NM-HDV2-1T1/E1
 - NM-HD-1V
 - NM-HD-2V
 - NM-HD-2VE
- Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845 with the EVM-HD-8FXS/DID module

For updates on voice gateways that support TICDSP5510 and updates on DSP technology, see Cisco.com. For more information, see *DSP Voice Quality Metrics Guide* at this URL:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/vqmetric.html

To enable voice quality statistics on the voice gateway, use this command:

```
mgcp voice-quality-stat all
```



Note

A warning message might be displayed advising that “enable voice stats might impact performance”.

For more information, see *Cisco IOS Voice Command Reference* at this URL:

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html

Supported Cisco 1040 Binary Image Files

Only the SvcMonAA2_42.img binary image file is supported for use on Cisco 1040 Sensors while using Service Monitor 2.1. After you install Service Monitor 2.1, the SvcMonAA2_42.img binary image file is available in the *NMSROOT*\ImageDir folder. To load the image onto sensors, see *Quick Start Guide for Cisco Unified Service Monitor 2.1*.



Note

NMSROOT is the directory in which Service Monitor was installed. The default value for NMSROOT is C:\Program Files\CSCOpX.



Caution

Installing binary image files other than SvcMonAA2_42.img can cause severe problems.

Known and Resolved Problems



Note

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

[Table 6](#) describes problems known to exist in this release; for resolved problems, see [Table 7](#).

Table 6 Known Problems in Service Monitor 2.1

Bug ID	Summary	Explanation
CSCsj91958	SM does not report endpoint properly for intercluster call	<p>In CVTQ reports, you will see the following as endpoints:</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Customer Voice Portal • Cisco Unified Presence Server <p>even though the RTP media stream does not flow to the them as they are used only for signaling.</p> <p>This occurs in Cisco Unified Service Monitor 2.1 and earlier versions.</p> <p>There is no workaround.</p>
CSCsv50189	Service Monitor 2.1 QOVR process uses too much CPU	<p>High CPU usage is observed on the Cisco Unified Operations Manager server; the offending process is cwjava. The output of pdshow shows that the PID of this cwjava process relates to the QOVR process.</p> <p>This has been observed on servers where:</p> <ul style="list-style-type: none"> • Operations Manager and Service Monitor are both running. • Service Monitor alone is running. <p>Workaround:</p> <p>Apply the patch that can be downloaded from Cisco.com. (The patch provides a replacement axis.jar file.)</p> <ol style="list-style-type: none"> 1. Log into Cisco.com. 2. Copy this URL to your browser and go: <code>http://www.cisco.com/cgi-bin/tablebuild.pl/servmon</code> 3. Download the patch and the readme for “CSCsv50189 for Cisco Unified Service Monitor 2.1”. 4. Follow the instructions in the readme file (README_CSCsv50189-1.0.txt) to install the patch.
CSCsr87157	Partial data in Top N report after QOVR restart	<p>If you restart the QOVR process, data for Top N reports from 12:00 a.m. until the time that you restarted the process is lost. The next day, when the Top N reports are generated, calculations use the available data which was collected between the time of the restart and the end of the day (11:59 p.m.).</p> <p>This happens only when Service Monitor is installed in a location other than the default (C:\Program Files\CSCOPx).</p> <p>Workaround:</p> <p>Install Service Monitor in the default location or do not restart the QOVR process if you particularly need the correct Top N data that day.</p>

Table 6 Known Problems in Service Monitor 2.1 (continued)

Bug ID	Summary	Explanation
CSCsr54308	MOH streams erroneously reported as calls with packet loss	<p>Cisco 1040 Sensors report on all RTP streams, including IP multicast streams. It has been observed that:</p> <ul style="list-style-type: none"> Streams from a Music On Hold (MOH) server using IP multicast might reuse the UDP ports and RTP SSRC header information. Because MOH streams might be intermittent—depending on the number of clients in an on-hold state—the 1040 might erroneously report that such streams are experiencing packet loss. <p>As a result, the MOH server appears in Service Monitor sensor reports in the Speaker column showing packet loss.</p> <p>Workaround:</p> <p>In sensor reports, ignore report rows that display packet loss for an MOH server. Use this information to identify the report rows to ignore:</p> <ul style="list-style-type: none"> The Speaker IP address is usually the MOH server IP address. The Listener IP address is usually 239.n.n.n.
CSCso79417	Device type and name are N/A in sensor report after changing IP address	<p>When a call occurs to or from a specific directory number (DN) and IP address, the correct device type and name appear in a sensor report until you change the IP address for the DN. After that, if you run a sensor report for the DN and the original IP address, the report displays N/A for the device type and name.</p> <p>There is no workaround for this problem.</p>
CSCso79022	Device type is N/A when CVTQ report generated after 30 minutes	<p>In some circumstances, the correct device type appears initially in a CVTQ report. If the report is generated again later, the report displays N/A for the device type.</p> <p>This has been observed as follows.</p> <ol style="list-style-type: none"> An analog phone is connected to a Cisco VG224 analog gateway. The gateway is registered to a Unified Communications Manager 5.x and the analog phone is registered to the same Unified Communications Manager. A 22-second call occurs from the analog phone (56003) to an IP phone (5001112). 15 minutes later, a user generates the CVTQ report. The correct device type appears in the report. 30 minutes later, a user generates the CVTQ report. The device type N/A appears in the report. <p>There is no workaround for this problem.</p>

Table 6 Known Problems in Service Monitor 2.1 (continued)

Bug ID	Summary	Explanation
CSCso58789	CDR/CDRM DB field shows Success even though HTTP/S credentials failed	<p>When Unified Communications Manager Credentials status is Failure for HTTP/S credentials, Service Monitor cannot poll data from the Unified Communications Manager. This is true even when Success is displayed for the CDR/M credential status. This occurs for Unified Communications Manager 5.x and later.</p> <p>To work around this problem, perform these steps:</p> <ol style="list-style-type: none"> 1. Correct the DNS settings on the Service Monitor server. 2. From the Service Monitor Unified Communications Manager Credentials page, verify the credentials. (Select the Unified Communications Manager credentials and click Verify.) 3. Confirm that the status displayed for both HTTP/S and CDR/M credentials is Success.
CSCsi71681	CVTQ, Sensor Reports don't show latest data when > 2000 records match	<p>Diagnostic reports display up to 2,000 rows. When you select report filters that match more than 2,000 records, the resulting report might not include all calls sequentially.</p> <p>To work around this problem, export the report to a CSV file; up to 30,000 rows can be exported to a CSV file by default. (An administrator can configure Service Monitor to export up to 64,000 rows; see online help for more information.)</p> <p>If a CSV file contains exactly 30,000 or exactly 64,000 rows, it is very likely that there are additional records that match the report filters. If this is the case:</p> <ul style="list-style-type: none"> • The CSV file still might not include all calls sequentially. • It is strongly recommended that you make the report filter more specific to match fewer records. Diagnostic reports are not designed to display all calls made in the system.
CSCsi85940	Handle leak with deleted sensors	<p>After you delete a sensor from Service Monitor, system resource usage on the Service Monitor server increases continuously while the sensor is on the network and attempting to communicate with a Service Monitor.</p> <p>Workaround:</p> <p>To prevent this problem, do one of the following before you delete a sensor:</p> <ul style="list-style-type: none"> • If you plan to add the sensor to another licensed instance of Service Monitor, do so and ensure that the sensor is communicating with that Service Monitor. • Shut these ports on the switch: <ul style="list-style-type: none"> – The port that physically connects to the 10/100-1 Fast Ethernet port on the sensor. – The SPAN or RSPAN destination port. (Alternatively, you can reconfigure this port so that it is no longer a SPAN or RSPAN destination port.)

Table 6 Known Problems in Service Monitor 2.1 (continued)

Bug ID	Summary	Explanation
CSCsi86375	Diagnostic report data incorrect for some nondirect calls	<p>For some nondirect calls, diagnostic (sensor and CVTQ) reports might include information that is incomplete. The circumstances and the problems that have been observed include:</p> <ul style="list-style-type: none"> • Using Music On Hold: <ol style="list-style-type: none"> 1. Two Cisco Unified IP Phones are registered with a Unified Communications Manager. 2. A call is placed between the phones. 3. One of the phones is placed on hold. <p>In this case, the sensor and CVTQ reports include records for:</p> <ul style="list-style-type: none"> – Phone 1 to Phone 2—Includes correct data. – Phone 2 to Phone 1—Includes correct data. – Unified Communications Manager (Music on Hold) to Phone 1—Speaker device type is Unavailable and speaker directory number is blank; speaker device type should be the IP address of the Unified Communications Manager. (In CVTQ reports only, there is no matching record for Unified Communications Manager to Phone 1 while on hold.) • Converting from a conference call to a direct call (after all but two phones drop out of a conference call). In CVTQ reports: <ul style="list-style-type: none"> – Records for the calls that dropped out of the conference call are correct. – Records for the last two phones can be written in combinations such as these: <p>Phone 1 to conference bridge; Phone 2 to Phone 1</p> <p>Phone 1 to Phone 2; Phone 2 to conference bridge</p> <p>Phone 1 to Phone 2; Phone 2 to Phone 1</p> <p>In the first two cases, the records for both sides of the call do not match. In the third case, there is no way to tell that these phones were ever in a conference call.</p> <p>There is no workaround for this problem.</p>
CSCsi66458	Cluster deleted in verifying state doesn't get deleted	<p>If you delete credentials for a Unified Communications Manager while the Last Contact Status is Verifying and the verification fails, the credential reappears as Failed.</p> <p>To work around this problem, do not delete a credential that is in Verifying state; wait until the Last Contact Status displays one of the final states: Failure, Success, or Waiting For Data.</p>

Table 6 Known Problems in Service Monitor 2.1 (continued)

Bug ID	Summary	Explanation
CSCsj45638	Editing Cisco 1040 Sensor configuration files causes problems	<p>If you edit a sensor configuration file, some editing applications might append a carriage-return character to each line. The sensor interprets the Windows carriage return character as part of the binary image filename. As a result, after every reset, the sensor tries to download and install the image from the TFTP server and fails. Hence, the sensor is not able to install a new image.</p> <p>Workaround:</p> <p>To open a sensor configuration file with an editing application, use Notepad. Notepad does not add carriage-return characters to each line.</p>
—	Monitored phone count can lag device discovery	<p>There might be a lag of up to one minute between the time that Service Monitor discovers devices and the time when the monitored phone count is updated.</p> <p>Workaround:</p> <p>There is no workaround for this problem.</p>

Table 7 describes problems resolved since the previous release of Service Monitor.

Table 7 Problems Resolved in Service Monitor 2.1

Bug ID	Summary	Additional Information
CSCsk77070	No CVTQ data from MGCP gateway	—
CSCso65632	Installation sometimes corrupts because DEP is not suppressed	—
CSCsc19066	Cisco 1040 does not generate syslog messages for Audio Codec G722	These problems are resolved by installing the SvcMonAA2_42.img binary image file that is available in Service Monitor 2.1
CSCsk61142	Ensure PLC (packet loss concealment) is emulated when grading G.711 MOS	
CSCsk98595	Ability to handle recurring streams	
CSCsl21586	MOS does NOT drop below 2.7 with 41.img even with high packet loss	

Documentation Updates

The following updates were not included in online help. They are included in *User Guide for Cisco Unified Service Monitor 2.1* on Cisco.com.

Additions

The following information is missing from the online help.

Backing Up Service Monitor Files

Service Monitor backup procedures back up the database only. To maintain a copy of sensor configuration files and any other files that you want to preserve, back them up from the Service Monitor server using whatever method you normally use. Service Monitor stores sensor configuration files (*.CNF) in the *NMSROOT\ImageDir* directory and stores sensor archive files—if archiving is enabled—in the *NMSROOT\DataDir* directory.

Corrections

In online help, the topic below incorrectly states that you should select the Resend on Failure checkbox to prevent Cisco Unified Communications Manager from sending outdated data to Service Monitor. Instead you should uncheck the Resend on Failure check box. The corrected text—in step 4—is included below.

Adding Service Monitor to Unified Communications Manager 5.x (or 6.x or 7.x) as a Billing Server



Note

- Perform this task on Unified Communications Manager version 5.x, 6.x, and 7.x only.
- Perform this task only while Service Monitor is up and running.

1. Launch Unified Communications Manager Serviceability.
2. Select **Tools > CDR Management**.
3. Scroll down to Billing Applications Server Parameters and click **Add New**.
4. Enter the following:
 - Host Name / IP Address—Enter the IP address of the system where Cisco Unified Service Monitor is installed.
 - User Name—Enter smuser.



Note Do not enter any username other than smuser.

- Password—Enter a password. The default password is smuser. To change this password: Change it in Service Monitor first.
Enter the same password that you entered for smuser while configuring other settings in Service Monitor.



Note If you changed the password in Service Monitor and Unified Communications Manager does not immediately accept the new password, wait one minute and enter the new password again.

- Select SFTP Protocol.
- Directory Path—Enter /home/smuser/.



Note Do not enter any directory path other than /home/smuser.

- Resend on Failure (Displayed in Unified Communications Manager 7.0 and later)—Uncheck this check box.

5. Click **Add**.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008-2009 Cisco Systems, Inc. All rights reserved.