Cisco TelePresence MCU Series 4.5(1.97)

Software Maintenance Release Notes
May 2018

Product Documentation

Version 4.5(1.97) is a maintenance release of software version 4.5 supported by the following MCU hardware platforms:

- Cisco TelePresence MCU MSE Series
- Cisco TelePresence MCU 5300 Series

The products are generically referred to as "the MCU" in this document.

The following links provide user documentation giving guidance on installation, initial configuration, and operation of the products:

- Cisco TelePresence MCU MSE Series
- Cisco TelePresence MCU 5300 Series

New Features in 4.5

Version 4.5 introduces some new features to extend and improve the conference experience.

The user interface and API have been updated as required to support these new features.

Table 1 New Feature Support

New Feature	MCU MSE 8510	MCU 5300 Series	MCU 4500 Series	MCU 4200 Series / MCU MSE 8420
Cisco ClearPath Support, page 3	Yes	Yes	No	No
Separate Content Channel Support for Encrypted SIP Participants, page 3	Yes	Yes	Yes	No
SIP Configuration Improvements, page 3	Yes	Yes	Yes	Yes
Disconnection of Inactive Calls, page 4	Yes	Yes	Yes	Yes
TMMBR Support, page 4	Yes	Yes	Yes	Yes
Cisco Call Home support, page 4	Yes	Yes	Yes	Yes
Isolated Media Processor Reboot , page 5	Yes	Yes	Yes	No
Improved Diagnostic Logging , page 5	Yes	Yes	Yes	Yes
New Console Commands to Return Additional System Information, page 6	Yes	Yes	Yes	Yes
New/Improved Methods for Feature Key Configuration, page 6	Yes	Yes	Yes	Yes
Online Help Format Updated, page 6	Yes	Yes	Yes	Yes

Cisco ClearPath Support

The MCU now supports ClearPath to improve media resilience within lossy networks.This feature is always enabled on the MCU MSE 8510 and MCU 5300 Series and does not require any configuration. The MCU implementation of ClearPath includes FEC (Forward Error Correction) and two other techniques which are only used inside the video streams, namely LTRF (Long Term Reference Frames) and incoming GDR (Gradual Decoder Refreshes).

ClearPath will be negotiated with any endpoints that support ClearPath. The MCU's web interface and API will report statistics and capabilities on the media resilience techniques used in those calls.

The following endpoints currently support ClearPath in their most recent software releases:

- Cisco Jabber Video for TelePresence
- Cisco Jabber
- Cisco TelePresence System T Series
- Cisco TelePresence System Quick Set Series (C20, SX20)
- Cisco TelePresence MX Series (MX200, MX300)
- Cisco TelePresence System EX Series (EX60, EX90)
- Cisco TelePresence Profile Series (Profile 42" , 52" , 52" Dual, 65" , and 65" Dual)
- Csco TelePresence Integrator C Series (Codecs C40, C60, and C90)

FEC (Forward Error Correction)

The MCU applies FEC to enable media packet recovery on outgoing video and audio streams. It can also process incoming streams containing FEC packets and will try to recover media packets lost from these streams.

The technique involves interleaving the original stream with additional, corrective packets, so that if media packets are lost they can potentially be recovered by the recipient without resorting to retransmission of the originals.

Applying FEC consumes additional bandwidth, so a call negotiated at a certain maximum bandwidth will use less bandwidth for the media streams because it needs overhead for the FEC packets. The bandwidth overhead can range from 0% – which means that FEC packets are not used – to 100% when every media packet is protected by a FEC packet. A 50% overhead means that one corrective packet is inserted to protect every two media packets.

The MCU only starts using FEC when it observes packet loss and then dynamically adjusts the overhead based on the monitored packet loss.

Separate Content Channel Support for Encrypted SIP Participants

This release introduces support for sending content in a separate channel from main video for encrypted SIP participants. Note that this functionality is already supported for H.323 participants and unencrypted SIP participants.

Support is limited to transcoded content and transcoded content channel in hybrid mode only; passthrough content is not supported to encrypted SIP participants.

This new feature is supported on all MCU platforms except MCU 4200 Series and MCU MSE 8420.

SIP Configuration Improvements

This release allows you to configure a box-wide default SIP domain for proxy/trunk calls. Previously this was only possible for registrar calls. For example, a typical use case would be an MCU trunked to a Cisco Unified Communications Manager (Unified CM), where you want to dial Unified CM registered endpoint numbers from the MCU and need a domain appended to the number before the call is placed over the Unified CM trunk.

This feature has introduced some new settings on the SIP settings page. The following new settings can now be configured on a boxwide basis via the **SIP settings** page:

- **Outbound call configuration** – this setting replaces the **SIP registrar usage** field. The drop-down menu now has three options:
  - *Use registrar* enables SIP registration and routes outbound SIP calls via the registrar.
  - *Use trunk* disables SIP registration and tears down existing registrations. Routes outbound calls to the trunk destination, e.g. Cisco VCS or Unified CM.
  - *Call direct* disables SIP registration and tears down existing registrations. Outbound SIP calls go directly (not via registrar or trunk).
- **Outbound address** – this setting replaces the **SIP proxy address** field. This field is the hostname or IP address of the SIP registrar or trunk destination.
- **Outbound domain** – this setting replaces the **SIP registrar domain** field. This field is the domain of the SIP registrar or trunk destination.

When upgrading to 4.5 from an earlier software version, the following fields will map accordingly after upgrade:

- if **SIP registrar usage** was set to *enabled*, the **Outbound call configuration** is set to *Use registrar*.
- if **SIP registrar usage** was set to *enabled* and both the **SIP registrar domain** and **SIP proxy address** filled in, the **SIP registrar** field is used to populate the **Outbound domain** and the the **SIP proxy address** is used to populate the **Outbound address**.
- if **SIP registrar usage** was set to *enabled* with only the **SIP registrar domain** filled in, the **SIP registrar domain** is used to populate both the **Outbound domain** and **outbound address**.
- if **SIP registrar usage** was set to *disabled* and the **SIP proxy address** filled in, the **Outbound call configuration** is set to *Use trunk*.
- if **SIP registrar usage** was set to *disabled* and the **SIP proxy address** filled in, the **SIP proxy address** is used to populate the **Outbound address**.
- if **SIP registrar usage** was set to *disabled* and a blank **SIP proxy address**, the **Outbound call configuration** is set to *Call direct*.

Note: When downgrading, any changes made post upgrade will be retained.

Disconnection of Inactive Calls

The MCU can now respond to inactive calls by disconnecting them. If media is expected from an endpoint but is not received for 30 to 45 seconds, then the MCU will disconnect the call.

When media has unexpectedly stopped in this way, the MCU will show last decoded frame to other participants in the conference until it disconnects the call.

This feature applies to any calls using H.323 or SIP call protocols. If auto-reconnect is enabled for the call, the MCU retries the call after disconnecting it.

The MCU will not disconnect a call if the endpoint has signaled that it is on hold or if the media channels are muted.

TMMBR Support

The MCU now supports flow control for SIP calls using RFC 5104 Temporary Maximum Media Stream Bit Rate Request (TMMBR). Flow control using TMMBR is supported for both incoming and outgoing main video and content channel.

Cisco Call Home support

This release enables the MCU to send diagnostic logs to the Cisco Call Home service. This feature can be configured to enable logs to be submitted automatically (disabled by default) or logs can be submitted manually.

Note: The MCU currently only supports anonymous reporting.

Logs are only sent via encrypted HTTPS connections. This requires the MCU to have an encryption feature key. Without this, you can view the Call Home web settings but the functionality will not be available.

Call Home messages are sent to `https://tools.cisco.com/its/service/oddce/services/DDCEService`. At that point, you may need to update your firewall to allow the reports through, by adding the domain `tools.cisco.com` and opening port 443 for outbound TCP traffic.

The MCU has a separate dedicated trust store to verify the connection to the Call Home server. (The MCU 4.5 has three trust stores - One for HTTPS connections, one for SIP connections and one for Call Home connections.) The MCU has a certificate pre-installed, however, it is possible to delete and upload new certificates. You can also reset the certificate to default.

The MCU can send 'inventory' data (i.e. basic system information such as serial number, hardware platform and software version) to the Call Home service. If automatic reporting is enabled, inventory data is sent each time the device starts up.

Device inventory reports are always available. Media resource or unit-wide diagnostic logs may also be available depending on whether an unexpected shutdown or media resource restart has occurred.

Note: If you have any questions about a Call Home report please contact Cisco TAC.

The user interface has a new Call Home settings page (**Logs > Call Home**) to allow the MCU to be configured to send diagnostic logs automatically in the event of an unexpected restart. Logs can also be submitted manually from this page.

Two new warning banners are introduced in this release to display in the user interface in the event of an unexpected device restart or unexpected media resource restart. Both of these banners can be dismissed from the Call Home page.

Serviceability Improvements

This release introduces several improvements to the serviceability of the MCU, as follows:

Isolated Media Processor Reboot

The MCU (MCU 8510, MCU 5300 Series, and MCU 4500 Series) is now more resilient in the unusual circumstance of individual media processor failure. On the MCU, if a media processor fails it will not cause the whole device to fail. This means that the other parts of the device software can maintain the state of the conferences—except for the tasks performed by that particular processor—while recovering the processor gracefully.

Note that some participants may experience a loss of audio and/or video in the unlikely event of a media processor failure, although it should come back after a pause of about 30 seconds.

In the case of a processor failure, the MCU isolates the processor as well as it can, while rebooting the processor, as follows:

- The MCU tries to reallocate tasks from the failed processor to other media resources if available. Participants may see a glitch while the tasks are recovered.
- If there are no spare media resources available, the affected participants will experience a loss of audio and/or video but the calls will stay up while the affected processor reboots.
- The processor reboots in about 30 seconds and audio/video to the affected participants will resume.
- It is also possible for presentation in a conference to be stopped. The user will have to re-initiate presentation manually in this case.

Improved Diagnostic Logging

This release features increased diagnostic detail, particularly in the core system and media processing software, which is continuously monitored and, in the event of a failure, stored for troubleshooting purposes.

After a failure, the diagnostic log can be retrieved via the web interface.

The improved diagnostics include:

- Additional detail and information in the diagnostic logs.
- More detailed event log messages.
- Improved Cisco TAC diagnostic options in the event of system failures.

New Console Commands to Return Additional System Information

This release introduces (on all MCU platforms) two new console commands that return additional system information. The commands are:

- **`show inventory`** console command (previously only available on the MCU 5300 Series) returns:
  - Model
  - Serial number
- **`show version`** console command returns:
  - Model
  - Currently installed software version
  - Current time
  - Uptime

New/Improved Methods for Feature Key Configuration

This release introduces some new/improved methods for configuring feature keys. These new methods can be done via console command and API.

The new console command is: **`feature_key list`** which returns a list of currently installed feature/license keys and their expiry dates.

Online Help Format Updated

This release introduces an updated format for the Help system and includes a table of contents to aid navigation.

Resolved and Open Issues in 4.5(1.97)

Use the links below to find up-to-date information about issues resolved since version 4.5(1.97), and open issues in this version, in the Cisco Bug Search Tool.

Issue Type	Link
Resolved Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613667&rls=4.5(1.97)&sb=fr&bt=custV
Open Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284183237&sb=afr&sts=open&svr=5nH&bt=custV

Limitations

Downgrade Without Restore Causes Username Inconsistency After Upgrade

When you downgrade from MCU 4.5 to MCU 4.3 or earlier, change a username, then upgrade to 4.5 again, that username's original 4.5 value is retained and is not changed. The reason for this is that the 4.4 software introduced a new field in configuration.xml to hold a longer username than was previously possible, but the previous field was also retained (the previous field was retained to ensure you could log in to restore your configuration). After you

downgrade, the new field remains in the configuration file until you overwrite it with your 4.3 (or earlier) configuration file. If you fail to restore your 4.3 (or earlier) configuration, the upgrade process does not subsequently recreate the configuration file (which already has the new field) and so the usernames can become inconsistent.

To work around this limitation, follow the recommended backup and restore procedures when downgrading or upgrading. When you downgrade, you must also restore your configuration to ensure that the configuration file matches the software version.

Google Chrome on Microsoft Windows 7 Fails to Provide Client Certificate

Certificate-based authentication and login will fail if the user attempts to access the MCU web interface using Google Chrome on Microsoft Windows 7. This issue only occurs when the client certificate is generated by the Microsoft Certification Authority. To work around the issue, use a different browser, operating system, or certification authority.

Transferring a Persistent Call can Result in Both Endpoints joining the Conference

When you transfer a persistent call from the active endpoint to another endpoint, the MCU redials the original endpoint, maintaining the persistence on that call, and also joins the target endpoint to the conference without call persistence. The transfer use case is not officially supported in this version.

Firefox 14

Firefox 14 is not supported for use with the MCU. We strongly recommend that you refrain from using Firefox 14 to access the MCU web interface. This version of the browser causes an issue that was not present in previous browser versions and which has been fixed in the following version (Firefox 15).

Dynamic IP Address Assignment

This limitation applies to MCU 4200 Series and MCU 4500 Series only. When you configure dynamic IP address assignment for IPv4 or IPv6 on one of the unit's Ethernet ports, the other IP interface on that port temporarily loses network connectivity.

Issues when Removing the CompactFlash™ During Operation

Removing the CompactFlash card while the MCU is in operation has been known to cause a restart.

Windows Media Player

Streaming a conference with Windows Media Player in multiple windows or tabs on the same browser will crash the browser. This is a known issue with Windows Media Player. If you need to stream more than one conference simultaneously, use a different player such as QuickTime or Real Player.

In addition, Windows Media Player 11 can display streams incorrectly when used as an embedded player with browsers other than Internet Explorer. This is a known incompatibility. In some cases, setting the video size of the main streaming video window (the Video size field in the Streaming page) to Large will correct the problem. To work around this issue, you can use QuickTime or RealPlayer instead of WMP, or use Internet Explorer instead of your normal browser.

The MCU does not support 64-bit versions of Windows Media Player. To work around this limitation, use a 32-bit version of Windows Media Player.

Streaming to QuickTime 7 Causes Problems with Some Browsers

Streaming to an embedded QuickTime player using the QuickTime 7.0 plus later option for the Player format on the MCU can cause certain browsers to crash or remain in the 'negotiating' state indefinitely. Affected browsers include: IE6; Firefox 1.5 (Mac and PC); Safari 2.0.3 and earlier, and Camino. IE7 and Safari 2.0.4 do not appear to be affected

by this. Using the QuickTime 6.5 plus later option for the Player format on the MCU will allow streaming to QuickTime using any browser that supports a QuickTime plug-in.

Clustering Limitations

Cisco TelePresence MCU Conference Director will only work with the master blade in a cluster.

If you are using Cisco Telepresence Management Server Version 12.6 or earlier to schedule conferences on clustered blades, only add the master blade to TMS. Do not add slave blades to TMS and remove from TMS any blade that you subsequently configure as a slave blade: you will need to reconfigure any scheduled conferences that were previously configured on slave blades as new conferences running on the master blade.

Uploading and Downloading Large Files while Heavily Loaded

We recommend that you do not upload or download large files from the MCU while it is hosting active calls. Files such as CDRs, audit logs and code images should be transferred when there are few or no calls on the MCU.

Automatic Link-Local IPv6 Assignment on Disabled Interface

When you enable IPv6 on any of the device's Ethernet ports (**Network > Port A** or **Network > Port B**), the device automatically assigns a link-local IPv6 address to each Ethernet port, even if the port is disabled. An IP address that is assigned to a disabled Ethernet port may not be apparent on the web interface.

Link-Local Addresses

Link-local IPv6 addresses are generated using the MAC address of each physical interface, and are thus unique per physical interface. No restrictions are imposed on link-local IPv6 addresses and all services enabled on their corresponding global IPv6 addresses are available on the link-local address. They support basic configuration and administration services (such as the web interface) but may not support full functionality such as making and receiving calls. Full functionality is only guaranteed for the main global IPv6 address on each interface.

We recommend using a PC with a single network interface connected to the local subnet when trying to access the MCU web UI using its link-local IPv6 address. Otherwise, login may fail since web browsers do not support URL redirection for an address with a scope ID.

MCU to MCU SIP Cascading is not Supported

When doing SIP to SIP cascading, the MCU's BFCP negotiation fails and the content appears in the main video instead of separate channel.

ClearPath not Supported on the Content Channel

MCU does not support ClearPath for the content channel.

Unicode H.323 IDs are Not Rendered Correctly on Conference Pages

Unicode H.323 IDs are not rendered correctly on conference pages. Additionally calls to or from endpoints that use UCS2 unicode H.323 IDs will not work.

Busy Message not sent when Port Limit is Reached

The MCU returns a TRYING message once the port limit is reached instead of a 486 busy message. This is only an issue when MCU is directly trunked from Cisco Unified Communications Manager. We recommend deploying the MCU (s) behind Cisco TelePresence Conductor to avoid this.

The MCU does not Support Sender-Side Flow Control

The MCU does not support sender-side media flow control. This can create problems when calls are made over low bandwidth pipes to endpoints that do not support receive-side flow control. In such calls, flow control is not possible for the media from the MCU to the endpoint. To assist in this situation low bandwidth can be set on the endpoint.

Unable to Add a VNC User on Windows 7 for MCU

It is not possible to add a VNC user to an MCU conference if the VNC user is running Windows 7 on their desktop. This is an issue on the Microsoft side - the connection will attempt to call out but fail. In the MCU logs the following error message will appear: `Connect failed with errno 60`. The workaround is for the VNC user to upgrade to Windows 7 SP1 and apply the necessary updates. (Issue identifier CSCun87357)

Slot 10 of the Cisco TelePresence MSE 8000 Chassis does not Support Clustering

Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering in this MCU software release. However, slot 10 in the same chassis as a cluster can be used for a standalone blade of any type. (Issue identifier CSCtr53874)

MCU Times Out Outbound SIP Call After 64 seconds

If an outbound SIP call from an MCU takes longer than 64 seconds to connect, the MCU may time-out the call before call set-up is complete. (Issue identifier CSCum70556) . To work around this:

- Reduce the call setup time by reconfiguring other nodes in the call path, or
- Use H.323, which has a longer timeout. (The Cisco TelePresence VCS can interwork between H.323 and SIP.)

Windows Media Player Streaming Only Works Over HTTP

Windows Media Player (WMP) streaming will work if the protocol is set to HTTP or Auto-negotiate, but there may be a delay in connection for auto-negotiate. MMS streaming will fail, and has also been removed from WMP 11 and onwards.

Direct Access of Page URLs can Result in Error Messages in Logs

In 4.5 (1.85), a "**Failed to write CSRF data for form <web page>**" error message is displayed in the logs, when you skip the login or the home page and access the Streaming page (<MCU IP>/streaming.html) or the Conference page (<MCUIP>/conference_list.html) directly. This error message occurs due to non-availability of cookie, if accessed using the url. This is not seen when the Streaming page or Conference page is loaded, by clicking on the links in login or Home page and does not impact the CSRF functionality.

Packet Loss and Video Degradation Issue in MCU

Packet loss and video degradation issue has been found for an MCU, which is up and running continuously for more than 828 days. We recommend to upgrade to later release versions and reboot the MCU as part of the upgrade.

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Upgrading to 4.5

Prerequisites

The software upgrade process requires a hardware restart. Schedule a downtime window and notify users of when the service will be unavailable. The duration of an upgrade can be up to 25 minutes.

Have the following available and complete the backup processes described before you proceed to upgrade the software:

- New software package.
- Current software image file (in case you need to reverse the upgrade).
- Back up of the configuration (the configuration.xml file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If using Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Administrative access to all units to be upgraded.
- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

Caution: Make sure that all the backup processes described in this section have been completed before you start the upgrade. Failure to do so could result in data loss.

Caution: If you are upgrading a cluster you must upgrade all blades in the cluster to the same software version.

Backup Configuration Instructions

Using a Web Browser

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Settings > Upgrade.**
4. In the **Backup and restore** area, click **Save backup file**.
5. Copy the resulting *configuration.xml* file to a secure location.

CAUTION: You must remember the administrator user name and password for the configuration backup file in case you ever need to use the backup.

Upgrade Instructions

Using a Web Browser

1. Unzip the image file locally.
2. In a web browser, navigate to the web interface of the device.

3. Sign in as an administrator.

   The username is *admin* and there is no password on a new unit.
4. Go to **Settings > Upgrade**.
5. In the **Main software image** section, locate the **New image file** field. Browse to and select the unzipped new image file.
6. Click **Upload software image**.

   The web browser uploads the file to the device, which may take a few minutes.

   Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process – this will cause the upload to fail.

   A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.
7. Click **Shut down MCU**. This option will now change to **Confirm MCU shutdown**. Click to confirm.
8. Click **Restart MCU and upgrade**.

   The unit will reboot and upgrade itself; this can take up to 25 minutes.

   Note: You may be logged out due to inactivity. If this happens, log in again, go to **Settings > Shutdown** and click **Restart MCU and upgrade**.
9. Go to the **Status** page to verify that your device is using the new version.
10. If necessary, restore your configuration; refer to the online help for details.

Note: You can monitor the upgrade progress via the serial port.

Downgrade Instructions

Note: We do not support downgrading MCU 5300 Series to any version earlier than 4.4(3.57). Please consult Cisco Technical Assistance Center if you require further assistance.

If you need to reverse your upgrade, you can re-install the former version of the software. The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

CAUTION: Make sure that all relevant backup processes described in Prerequisites have been completed before you start the downgrade. Failure to do so could result in data loss.

Downgrade Procedure

You need the correct version of the software and your corresponding saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Restart the hardware and check the status via the web interface.
   The status report indicates the software version.
3. Restore your configuration from the saved XML file; refer to the online help for details.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.

3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Document Revision History

Date	Revision	Description
May 2018	09	Content update
April 2018	09	Seventh maintenance release version
October 2017	08	Sixth maintenance release version
February 2017	07	Fifth maintenance release version
November 2016	06	Fifth maintenance release version
March 2016	05	Fourth maintenance release version
August 2015	04	Third maintenance release version
July 2015	03	Second maintenance release version
November 2014	02	First maintenance release version
June 2014	01	Release version

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)