Cisco TelePresence Server 4.3(1.14)

Release Notes

First Published: April 2016

Last Updated: July 2016

Product Documentation

The following sites contain documents covering installation, initial configuration, and operation of the product:

- Release notes: http://www.cisco.com/en/US/products/ps11339/prod_release_notes_list.html
- Install guides: http://www.cisco.com/en/US/products/ps11339/prod_installation_guides_list.html
- Configuration guides: http://www.cisco.com/en/US/products/ps11339/products_installation_and_configuration_guides_list.html
- API reference guides: http://www.cisco.com/en/US/products/ps11339/products_programming_reference_guides_list.html
- Maintain and operate guides: http://www.cisco.com/en/US/products/ps11339/prod_maintenance_guides_list.html
- Licensing information: http://www.cisco.com/en/US/products/ps11339/products_licensing_information_listing.html

New Features in 4.3(1.14)

Version 4.3(1.14) is a maintenance release. For more information, see Resolved and Open Issues, page 5.

Version 4.3(1.13) introduced some new features to extend and improve the conference experience. This release is available on all TelePresence Server platforms, including the Cisco TelePresence Server on Multiparty Media 820.

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

Table 1 New feature support by TelePresence Server platform

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
Cisco TelePresence Server on Virtual Machine improvements				
Media 410v Capacity Increase, page 2	No	No	Yes	No
Cisco TelePresence Server on Virtual Machine Operating System Changes, page 2	No	No	Yes	No

Table 1 New feature support by TelePresence Server platform (continued)

Feature name	7010 & MSE 8710	Media 310/320	Virtual Machine	Media 820
User experience improvements				
PIN Entry Retry Limit, page 2	Yes	Yes	Yes	Yes
New Default Lobby and PIN Entry Screens, page 2	Yes	Yes	Yes	Yes
New Default Voice Prompts, page 2	Yes	Yes	Yes	Yes
Custom Voice Prompts, page 3	Yes	Yes	Yes	Yes
In-call Presenter Icon, page 3	Yes	Yes	Yes	Yes
New Conference Entrance Flow, page 4	Yes	Yes	Yes	Yes
Custom Lobby Screen Background (Preview Feature), page 4	Yes	Yes	Yes	Yes

Cisco TelePresence Server on Virtual Machine Improvements

Media 410v Capacity Increase

The Cisco Multiparty Media 410v capacity increases from 27 screen licenses to 32. This is an 18.5% capacity improvement, equivalent to an increase from 54 to 64 720p calls. For further details, see Platform Licensing Comparison, page 6.

Cisco TelePresence Server on Virtual Machine Operating System Changes

The Cisco TelePresence Server on Virtual Machine has undergone platform operating system changes which require a re-deployment of the .ova rather than an upgrade. For further details, see Using 4.3(1.14) on the Cisco TelePresence Server on Virtual Machine, page 10.

The Cisco TelePresence Server on Virtual Machine now has a minimum requirement of 16 GB RAM. Previously the minimum requirement was 12 GB.

User Experience Improvements

This release features several User Experience improvements:

PIN Entry Retry Limit

If a PIN is entered incorrectly three times, the participant is told that they have entered the pin incorrectly too many times and is disconnected.

New Default Lobby and PIN Entry Screens

The default lobby screen and the PIN entry screen are updated to better match the CE endpoint portfolio.

New Default Voice Prompts

This release introduces new voice prompts and default prompts are provided for each. New voice prompts now appear at the following events:

- PIN entry
- PIN entry where guest PIN is blank

- Incorrect PIN entered
- PIN retry limit hit
- Welcome screen
- Only participant with chair privilege joins conference. If **Wait For Chair** is disabled the voice prompt will occur when any participant joins.
- Guest waiting for chair to join before conference start
- Exit lobby

Note: In addition to the new default prompts, Conductor allows you to specify other set languages. For more information, see the Cisco TelePresence Conductor Administrator Guide (XC4.2) at: http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-maintenance-guides-list.html.

Custom Voice Prompts

This feature allows you to localize the voice prompts into your own language. All voice prompts can be localized via the API.

The customized audio file must be:

- 16 bit
- 16 kHz sample rate
- WAV PCM format
- Maximum length 40 seconds
- Mono track

To add custom voice prompts:

1. Set up an HTTP server to host the audio file(s) using your preferred suitable option.
2. On TelePresence Conductor, go to **Conference Conguration > Conference Templates** and find the template for the conference.
3. Go to **Advanced parameters**, click **Edit**.
4. In the **Custom parameters** text box, enter the URL of the audio file using the appropriate API command as defined in the API Guide under `flex.conference.create` inputs.
5. Click **Save**.
6. We recommend that you test the setup at this point to make sure the system works as expected.

Note: TelePresence Conductor can accept the customization field and dial into and start the conference but this does not guarantee that the customized audio prompts are heard. If errors occur when TelePresence Server tries to retrieve and play back a prompt, then no prompt will be played and silence will be heard.

In-call Presenter Icon

When a presentation is being shared, all calls now see a small icon next to the name label to indicate the presenter in the PiP strip.

Note: The icon does not show at resolutions below 288p.

New Conference Entrance Flow

The experience of joining a conference has been improved. The lobby screen duration is reduced from five seconds to three, and participants who join via a PIN entry screen now only see a welcome screen if there is a customized welcome screen message set.

Custom Lobby Screen Background (Preview Feature)

Custom Lobby Screen Disclaimer

The custom lobby screen background feature in TelePresence Server is provided as a preview feature and is not intended for use in production environments. Use of this feature is subject to the software license and limited warranty http://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html for TelePresence Server. Cisco reserves the right to disable the custom lobby screen background feature at any time without notice. Cisco Technical Support will provide limited assistance to customers who wish to use the custom lobby screen background feature.

Description

This preview feature can be used to display a customized background if for instance you want to incorporate a company logo.

A separate background image can be configured for each conference. A maximum of five customized images can be used on a single TelePresence Server simultaneously. If the limit is exceeded, then the `conference.create` API command to TelePresence Server will fail and the conference will not be usable. To ensure this doesn't happen we recommend that you have no more than five images per TelePresence Conductor.

The image needs to be: PNG format, 1920 x 1080 resolution, 5 MB max file size. The files must be held on an external HTTP web server.

To use this feature, the Administrator needs to enter the API field (`customBackgroundImageURL`) with the URL of the background image file into the Custom Parameters field in the Advanced Parameter section of the Conference Template on TelePresence Conductor.

For further information on implementing this preview feature, please contact your Cisco TAC representative for the Design Guidelines and Instructions.

Changes and Minor Enhancements

Change to the Number of Video Streams for Multistream

This release introduces a change to the number of video streams transmitted by TelePresence Server to multistream-capable endpoints. It can now transmit up to 18 video streams to an endpoint. Previously it was 16 video streams.

Notice of Deprecation

Locally Managed Mode

TelePresence Server 4.2 was the last release to support Locally managed mode. From this release, 4.3(1.14) onwards Locally managed mode is no longer supported.

TelePresence Conductor is required to support the latest TelePresence Server releases and features.

Cisco has not announced or started the end of life process for the TelePresence Server 4.x software, when it does it will follow the standard process for maintenance releases and TAC support.

Half Duplex Mode

From this release, 4.3(1.14) onwards, half duplex Ethernet mode is no longer supported.

Resolved and Open Issues

Resolved Issues

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&rls=4.3%281.14%29&sb=fr&sts=fd&svr=5nH&srtBy=byRel&bt=empCustV

Open Issues

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613665&sb=afr&sts=open&svr=5nH&bt=empCustV

Platform Licensing Comparison

The following table compares the number of TelePresence Server screen licenses that each of the platforms can accept and how they translate into conferencing capacity.

Note: These are the recommended combinations for configuration via TelePresence Conductor. Other combinations are possible but are likely to cost more than expected. For further information see http://docwiki.cisco.com/wiki/Advanced_Resource_Optimization_on_TelePresence_Server.

Table 2 TelePresence Server screen licenses per call for each call type

Call type description			Screen licenses required per call
Main video	Audio	Content	
-	Mono	-	1/52
360p30†	Mono	In main video	⅛
360p30†	Stereo	720p5	¼
480p30	Stereo	In main video	¼
480p30	Stereo	720p5	⅓
720p30	Stereo	720p5	½
720p30	Stereo	720p30	1
1080p30	Stereo	720p15	1
720p60	Stereo	720p15	1
1080p30	Stereo	720p30	1½
Three-screen 720p30	Multichannel	720p5	1½
Three-screen 720p30	Multichannel	720p30	2
1080p30	Stereo	1080p30	2
Dual-screen 1080p30	Stereo	720p30	2
Three-screen 1080p	Multichannel	720p30	3
Three-screen 1080p	Multichannel	1080p30	4
Four-screen 1080p	Stereo	1080p30	4

† Requires TelePresence Conductor XC2.2 or later.

Table 3 TelePresence Server conferencing capacity on various platforms for current products

Screen licenses required per call	Maximum calls by hardware type (with licenses to provide 100% of capacity)								
	8 Cores VM (8 vCPU)	Media 310 or MCU 5310	30 vCPU VM ‡	Media 320 or MCU 5320	Two appliance cluster	Media 820	Media 410v ‡ (46 vCPU)	Four blade cluster with 8710/8510	Two blade cluster with Media 820
	5 screen licenses	6 screen licenses	10 screen licenses	12 screen licenses	24 screen licenses	30 screen licenses	32 screen licenses	48 screen licenses	60 screen licenses
1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*
⅛	41	49	81	97	195	200*	200*	200*	200*
¼	20	24	40	48	97	120	128	195	200*
⅓	15	18	30	36	73	90	96	146	180
½	10	12	20	24	48	60	64	97	120
1	5	6	10	12	24	30	32	48	60
1½	3	4	6	8	16	20	21	32	40
2	2	3	5	6	12	15	16	24	30
3	1	2	3	4	8	10	10	16	20
4	1	1	2	3	6	7	8	12	15

* 200 is the maximum number of calls on a TelePresence Server. Requires Cisco TelePresence Conductor XC2.3 or later.

‡ To achieve the maximum number of calls, Cisco TelePresence Server on Virtual Machine must be the only VM hosted on the Multiparty Media 410v or 30 vCPU VM. It cannot be co-resident with any other UC application (unlike the 8-core option that runs at 2.4GHz minimum and can be co-resident).

Note: The table above assumes that calls of one type are being used to reach these maximum values. To calculate the total number of licenses required for a variety of concurrent calls, sum the screen licenses required for each concurrent call.

Note: BE6K has not had any capacity changes since 4.1(1.79).

Note: This table is for current products only. For a comprehensive list including older products please see the licensing capacity table in the online help.

Limitations

Flow Control Disabled for Endpoints that Negotiate TIP/MUX

Endpoints that negotiate TIP/MUX, including the CTS series, would have been negatively impacted by the new flow control algorithm introduced in TelePresence Server 4.0. Flow control requests have thus deliberately been disabled for TelePresence Server 4.0 or later when it is in calls with these endpoints. This also means that the **Received video: flow control on video errors** setting will have no effect if it is enabled for these endpoints.

The TelePresence Server Does Not Support Sender-Side Flow Control

The TelePresence Server does not currently 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 TelePresence Server to the endpoint. Issue identifier CSCun86953.

Video Issues with Earlier Versions of TX Endpoint Software

Note: We strongly recommend that you use TX6.0.5 or later software on these endpoints when they interoperate with TelePresence Server 3.1(1.95) or later.

The following endpoints display significant orange or green flashes when they are using software versions between TX6.0.0 and TX6.0.4 in calls with TelePresence Server 3.1(1.95) or later:

- Cisco TelePresence System 500-32
- Cisco TelePresence TX1300 Series
- Cisco TelePresence TX9000 Series
- Cisco TelePresence TX9200 Series

Call Transfer is Disabled

The TelePresence Server does not support call transfer.

DTLS and Custom Certificates

DTLS is used to negotiate encryption parameters with TIP endpoints. This requires a certificate to be used. There are some limitations when using DTLS with customer-supplied certificates:

- Opportunistic DTLS, as supported in release 2.2, always uses the default certificate for DTLS negotiation, even if a customer-supplied certificate is uploaded. This is due to technical limitations.
- Release 2.3 and later supports a new improved DTLS type – 'negotiated DTLS'. When using 'negotiated DTLS', the TelePresence Server uses the customer-supplied certificate if they have uploaded one (which is the preferred procedure). If 'negotiated DTLS' is used in a call to a CTS endpoint combined with some custom certificates, DTLS may fail on these calls. This is due to defect CSCts24503. The call may still connect but without encryption. As a workaround, use a smaller custom certificate such as a certificate with a 1024 byte key or use the default certificate on the TelePresence Server.

HD Quality Indicators on CTS Endpoints

The lobby screen is a static image that is designed for HD mode, that is, 720 pixels high. When a CTS endpoint displays the lobby screen, it may go on to incorrectly report the quality of the received video stream. The quality indicator may show four bars—for 720p video—even though the endpoint is actually receiving 1080p video and should display five bars.

Encryption Required Causes Issues with Some Endpoints

Some endpoints such as the Sony XG-80 and HG-90, and the TANDBERG Classic 6000s are unable to join conferences in which encryption is required, even when encryption is enabled on the endpoint. (TANDBERG is now part of Cisco.)

Setting these conferences to have optional encryption allows these endpoints to join using encryption.

Clustering Limitations

Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering for 8710 blades in this TelePresence Server software release. However, slot 10 in the same chassis as a cluster can be used for clustering Media 820 blades, or for standalone blades of any type.

TIP Calls and Encryption Required Conferences

TIP calls can only join conferences with the Encryption setting configured to *Required* when TLS encrypted signaling is used throughout the call signaling path. This ensures that the call is fully secure.

Recommended VCS Version X7.2 or Later

On calls to CTS endpoints in certain network configurations, calls may fail or become audio-only with earlier versions of VCS. In order to avoid this, upgrade VCS to X7.2. If using a custom zone profile on VCS for the Cisco Unified Communications Manager zone, ensure that **SIP UPDATE strip** mode is disabled on this zone.

Limited Support for some VM Operations

Snapshotting a Cisco TelePresence Server on Virtual Machine is not recommended and should only be undertaken when no calls are active and only when following the best practice guidelines from VMware. Cisco recommends that customers check for any automated snapshotting processes and disable them for any Cisco TelePresence Server on Virtual Machines.

Cloning of a Cisco TelePresence Server on Virtual Machine is not supported—any cloned machines will require new licenses.

Unless otherwise stated, Cisco supports only those VMware features recommended in this and other Cisco TelePresence Server on Virtual Machine guides.

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 4.3(1.14)

Prerequisites and Software Dependencies

Note: 8710, 7010, Media 320, Media 310, Media 820 can be upgraded as standard using the .kupgrade or .zupgrade files. Back up your configuration file before upgrading.

Using 4.3(1.14) on the Cisco TelePresence Server on Virtual Machine

To use any version of 4.3, the Cisco TelePresence Server on Virtual Machine needs to be redeployed using the .ova file. Cisco have provided an upgrade redeployment tool that ensures serial numbers are preserved, and thus all the keys (activation, encryption, screen licenses) are carried across to the new deployment.

Note: If you have already redeployed to 4.3(1.13) you can upgrade to 4.3(1.14) using the standard .tar.xz file.

Note: Once you have deployed a 4.3 Cisco TelePresence Server on Virtual Machine, you cannot downgrade to 4.2 or earlier. If you have kept the old 4.2 Cisco TelePresence Server on Virtual Machine VM, you can power that on (assuming you power down the 4.3 Cisco TelePresence Server on Virtual Machine VM) at any time and resume using it.

Deploying this release is similar to deploying previous versions of Cisco TelePresence Server on Virtual Machine except you have the additional option to use DHCP to acquire an IP address. To do this leave the IP address, Subnet mask and Default Gateway Properties blank when deploying the Cisco TelePresence Server on Virtual Machine.

Caution: You will need to get new activation and license keys if you redeploy without using the upgrade redeployment tool.

For more information on using the Cisco TelePresence Server on Virtual Machine Upgrade Redeployment Tool, see "Migrating to TelePresence Server on Virtual Machine 4.3", at: http://www.cisco.com/c/en/us/support/conferencing/telepresence-server/products-installation-guides-list.html.

Note: Before migrating your Cisco TelePresence Server on Virtual Machine to 4.3(1.14), ensure the host is running ESXi 5.5 update 2 (or later) or ESXi 6.0. You may be required to update your vCenter Server, please see: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&1=994,694,430,795,620&2=.

Software Dependencies

In the case of the TelePresence Server MSE 8710 blade(s) and the Media 820, the Cisco TelePresence Supervisor MSE 8050 blade must be running Supervisor software version 2.2 or later.

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.
  - For hardware platforms, this will be a file with a **.zip** extension, for example **cisco_ts_media_300_4.3_1.13.zip** for the Media 310/320 platforms. You must unzip this file before you can use it.
- Current software image file (in case you need to reverse the upgrade).
- Backup 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 members of the cluster to the same software version.

Note: While you are upgrading a cluster, or restarting it for another reason, the master cannot report the cluster's full capacity until the slaves have also restarted. Any devices that poll the master for such information should check that the slaves are back up before assuming that the capacity has permanently been reduced, or that there is some other fault in the cluster.

Backing Up Your Configuration

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Configuration > Upgrade**.
4. In the **Back up and restore** section, 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

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator and configure a new password, if required..
   The username is *admin*
3. Go to **Configuration > Upgrade**.
4. In the **Main software image** section, locate the **New image file** field. Browse to and select the new image file.
5. 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*.
6. Click **Shut down TelePresence Server**. This option will now change to **Confirm TelePresence Server shutdown**. Click to confirm.
7. Click **Restart TelePresence Server 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 **Configuration > Shutdown** and click **Restart TelePresence Server and upgrade**.
8. Go to the **Status** page to verify that your device is using the new version.
9. If necessary, restore your configuration; refer to the online help for details.

Downgrade Instructions

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, page 10 have been completed before you start the downgrade. Failure to do so could result in data loss.

Note: We recommend that you delete any custom certificate before downgrading on Media 310 and Media 320 platforms, and re-upload the certificate after downgrading.

Note: Cisco TelePresence Server on Virtual Machine will need to be redeployed. Back up your configuration file, then deploy using the .ova file. If using Screen Licensing instead of Multiparty Licensing, new Screen Licenses and Feature Keys will be needed unless you download your backed up licenses and keys.

Downgrading from 4.3(1.14)

You need the correct target version of the software and the 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

Table 4 TelePresence Server release notes revisions

Date	Description
July 2016	Addition of " Change to the Number of Video Streams for Multistream" (previously omitted)
June 2016	Version 4.3(1.14) MR1 release
April 2016	Addition of ESXi prerequisites for vTS migration.
April 2016	Version 4.3(1.13) First release

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)