Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 11.2(3)

First Published: 2019-01-30

Release Notes

Use these release notes with the following Cisco IP Phone 8800 Series Multiplatform Phones running SIP Firmware Release 11.2(3).

- Cisco IP Phone 8811, 8841, 8851, and 8861 Multiplatform Phones
- Cisco IP Phone 8845 and 8865 Multiplatform Phones

The following table describes the individual phone requirements.

Phone	Support Server
Cisco IP Phone 8800 Series Multiplatform Phones	BroadSoft BroadWorks 22.0 MetaSphere CFS version 9.4 Asterisk 11.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Phone 8800 Series Documentation

See the publications that are specific to your language, phone model, and multiplatform firmware release. Navigate from the following Uniform Resource Locator (URL):

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/index.html

New and Changed Features

BLF Configuration Enhancements

The Busy Lamp Field (BLF) feature enables you to monitor other users' lines. The following enhancements enable you to configure the BLF feature.

- If you have configured a BLF list for the phone, you can activate or deactivate monitoring of the entire list with the new **BLF List** setting. This setting is available on the **Attendant console preferences** menu of the phone. Setting it to **Show** activates monitoring of the BLF list. The phone assigns available line keys in sequence to monitor the BLF list entries, and starts showing the status of the monitored lines on

the BLF keys. You can also access this setting on the phone administration web page, in **Voice** > **Att Console** > **General**.

Note The **Use Line Keys For BLF List** setting has significance only when monitoring of the BLF list is active. This parameter controls whether the phone uses its own line keys for monitoring the BLF list. When it is set to **No**, the phone uses only the keys on any Key Expansion Module present for monitoring the BLF list.

- You can also configure line keys individually to monitor other users, if you allow it. Feature configuration on line keys has been enhanced to support BLF in addition to speed dial. Users can also add speed dial and call pick up to the BLF key configuration, if you allow these options. Use the new **Customizable PLK options** field in **Voice** > **Att Console** > **General** on the phone administration web page to control which options are allowed. To allow an option, add the option to this field. The speed dial option is added by default when you upgrade the phone firmware to this release, to keep the default behaviour of the phone consistent with the previous release.

  As in the previous release, you must disable line keys from functioning as extensions, to allow feature configuration on line keys on the phone. Also as in the previous release, you press and hold down a line key for two seconds to configure a feature on the line key.

  You can select any available line key to configure features. You can also select a line key that is functioning as a speed-dial key or as a BLF key. You cannot select keys on which you have configured other features.

  The phone subscribes to the BLF list URI that you specify, to be notified of changes in the status of monitored lines. If you do not specify a BLF list URI, the phone subscribes to `$USER@$PROXY`.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Catalan Language Support

You and your user can set the phones to display text in Catalan. On the phone administration web page, the **Locale** field in **Voice** > **Regional** contains the new **ca-ES** option.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Cisco Headset 521 and 522

The Cisco Headset 521 and 522 are two wired headsets that have been developed for use on Cisco IP Phones and devices. The Cisco Headset 521 features a single earpiece for extended wear and comfort. The Cisco Headset 522 features two earpieces for use in a noisy workplace.

Both headsets feature a 3.5-mm connector for use on laptops and mobile devices. An inline controller with a USB connector is also available for use on the Cisco IP Phone 8851, 8861, and 8865 with Multiplaform Firmware. The controller is an easy way to answer your calls, and to access basic phone features such as hold and resume, mute, and volume control.

On the phone screen, the user can customize the headset's sidetone, tune the speaker, adjust the microphone gain, and test the microphone.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*

Cisco Headset 561 and 562

The Cisco Headset 561 and 562 are two wireless headsets that are developed for Cisco products and services. The Cisco Headset 561 features a single earpiece, and offers lightweight comfort. The Cisco Headset 562 features two earpieces for use in a noisy environment or busy office.

The Cisco Headset 561 and 562 use a headset base to connect with Cisco IP Phones and charge the headsets. The headsets communicate with the base using Digital Enhanced Cordless Telecommunications (DECT).

The available options for the base are Standard base and Multibase. The Standard base supports connection with a single source from a phone or a computer. The Multibase supports multiple sources from phones, computers, and Bluetooth-paired devices, and provides an easy and intuitive switch among the connected sources.

The Cisco Headset 561 and 562 with Standard Base and Mulltibase connect to the phones with one of the cables:

- Y-cable (on the RJ9 port and the AUX port)
- USB cable (on the USB port)

On the phone screen, the user can customize the headset's sidetone, tune the speaker, adjust the microphone gain, and test the microphone.

Where to Find More Information

- Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide
- Cisco IP Phone 8800 Series Multiplatform Phones User Guide

Control of Phone Configuration Reporting

You can control when the phone reports its configuration to the provisioning server. This is in addition to the standard report upload that happens as part of the phone shutdown or restart.

Use the new **Report to Server** drop-down list on the phone administration web page, in **Voice** > **Provisioning** > **Upload Configuration Options**. When you choose **On Local Change**, the phone reports its configuration when any configuration parameter changes by an action on the phone or on the phone administration web page. The phone waits for a few seconds after a change is made, and then reports the configuration. This wait time is defined in the **Upload Delay On Local Change** field. Specify a value in number of seconds (10 minimum, 60 default, 900 maximum). This delay ensures that changes are reported to the web server in batches, rather than reporting a single change at a time.

Alternately, the phone can report its configuration at regular intervals. Choose **Periodically** in the **Report to Server** drop-down list. Then, in the **Periodic Upload to Server** field, specify an interval in number of seconds (600 minimum, 3600 default, 2592000 (30 days) maximum).

In all cases, the report rule that you specify defines the configuration report that the phone sends. Two report upload destination URLs are supported in the **Report Rule** field which provide flexibility in both destination and content of the uploaded report.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Device Identifier in Uploaded Syslog Messages

You can now choose to include a device identifier for the phone in syslog messages that are uploaded to the syslog server. While the IP address of a phone may change over time, the device identifier does not change. This can ease the process of identifying the source of each message in a stream of incoming messages from multiple phones. The device identifier appears after the timestamp in each message.

On the phone administration web page, you will see a new field named **Syslog Identifier** in **Voice** > **System** > **Optional Network Configuration**. You can also configure this setting in the XML configuration file. You can choose the type of device identifier to include:

- none
- the MAC address of the phone, in the standard colon-separated format, or as continuous upper case or lower case letters and digits
- the product serial number of the phone

This feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

DND and Call Forwarding Sync Between the Phone and the Server

Besides Feature Key Synchronization (FKS), you can also enable the do not disturb (DND) and call forwarding synchronization between the phone and the server through the XSI service. When both FKS and XSI Synchronization are enabled, FKS takes precedent over XSI Synchronization.

You use the new fields **DND Enable** and **CFWD Enable** on the phone administration web page to enable or disable this feature. When enabled, the settings of DND and call forwarding on the server are synchronized to the phone. The status changes made on the phone will also be synchronized to the server.

The fields are located in the **XSI Line Service** section from **Voice** > **Ext (n)**.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Key Expansion Modules for Cisco IP Phone 8851, 8861, and 8865

Firmware Release 11.2(3) introduces support for two new key expansion modules:

- Cisco IP Phone 8851/8861 Key Expansion Module—for the Cisco IP Phone 8851 and 8861(audio phones)
- Cisco IP Phone 8865 Key Expansion Module—for the Cisco IP Phone 8865(video phones)

The new expansion modules are supported on firmware Release 11.2(3) or later.

Both expansion modules feature a dual LCD screen, 14 line keys, 2 pages, and have a one-column display. They also have a light gray background that replaces the existing blue background found on the current key expansion module.

The new key expansion modules support the same features of the single-LCD key expansion module.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*

Phone Audio Compliance Standards

You can specify a compliance standard for the phone. When a compliance standard is specified, the acoustic parameters that conform to the specified standard are loaded to the phone.

You can specify the audio compliance standard from the phone administrator web page **Voice** > **User** > **Audio Compliance**. The options are: ETSI and TIA. TIA (A set of standards by Telecommunications Industry Association) is the default.

The feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 8800 Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Multiplatform Phones Provisioning Guide*

Profile Account Authentication

Profile account authentication enables the phone to resynchronize the provisioning profile. You can specify a profile authentication type for phone users to use.

The new field **Profile Authentication Type** replaces the **Profile Account Enable** field on the phone administration web page. The available options are: Disabled, Basic HTTP Authentication, and XSI Authentication.

When you disable this feature, the phone user can't enter the authentication account on the phone screen. When you specify an authentication type, the phone user can use the provided credentials to resynchronize the provisioning profile either when prompted or through the **Profile account setup** menu on the phone screen.

If **XSI Authentication** is specified as the authentication type, you can use either XSI login credentials or SIP credentials to resynchronize the provisioning profile. Logging into XSI server with SIP credentials requires Broadsoft Broadworks 20.0 or later versions.

To use SIP credentials, set **XSI Host Server**, **XSI Authentication Type** (as **SIP Credentials**), **SIP Auth ID**, and **SIP Password** in the **XSI Phone Service** section from the **Voice** > **Phone** tab on the phone administration web page.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*

RFC 8188-Based HTTP Content Encryption for Configuration Files

The phone now supports RFC 8188-based HTTP content encryption with AES-128-GCM ciphering for configuration files. With this encryption method, any entity can read the HTTP message headers. However, only the entities that know the Input Keying Material (IKM) can read the payload. When the phone is provisioned with the IKM, the phone and the provisioning server can exchange configuration files securely, while allowing third-party network elements to use the message headers for analytic and monitoring purposes.

The new XML configuration parameter **`IKM_HTTP_Encrypt_Content`** holds the IKM on the phone. For security reasons, this parameter is not accessible on the phone administration web page. It is also not visible in the phone's configuration file, which you can access from the phone's IP address or from the phone's configuration reports sent to the provisioning server.

Note The phone continues to support the AES-256-CBC encryption method. As in the previous release, you specify the AES-256-CBC key with the **`--key`** keyword in profile rules and report rules. Which of the two encryption and decryption methods the phone applies depends on the inputs that you provide.

If you want to use the RFC 8188-based encryption, ensure the following:

- Provision the phone with the IKM by specifying the IKM with the new XML parameter **`IKM_HTTP_Encrypt_Content`** in the configuration file that is sent from the provisioning server to the phone.
- If this encryption is applied to the configuration files sent from the provisioning server to the phone, ensure that the *Content-Encoding* HTTP header in the configuration file has “aes128gcm”.

  In the absence of this header, the AES-256-CBC method is given precedence. The phone applies AES-256-CBC decryption if a AES-256-CBC key is present in a profile rule, regardless of IKM.
- If you want the phone to apply this encryption to the configuration reports that it sends to the provisioning server, ensure that there is no AES-256-CBC key specified in the report rule.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Remotely Initiated Problem Reports

You can initiate a phone problem report remotely. To do this, initiate a `SIP-NOTIFY` message from the server to the phone, with the Event specified as `prt-gen`. The phone generates a problem report using the Cisco Problem Report Tool (PRT), with the problem description "Remote PRT Trigger". If you have configured an upload rule for problem reports, the phone also uploads the problem report according to the upload rule.

You can see the status of the most recent problem report initiation on the phone administration web page > **Info** > **Status**. A new section called **PRT Status** shows the location of initiation and the status of the report generation, and the status of the report upload.

You can access a remotely-initiated problem report from the same location as locally-initiated problem reports on the phone administration web page.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Support for Early Media and Preconditions

Your phone now supports early media negotiation and precondition signaling.

For an outgoing call, a SIP message from the phone includes the P-Early-Media header, which contains the status of the early media stream. If the status in the header is not indicating that the network is blocking the early media stream, the phone plays the early media instead of the ringback tone while waiting for the call to be connected.

Precondition signaling defers incoming call notifications until the phone receives the message that preconditions are satisfied to establish the call.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Contact Search in Multiple Directories

You can now search for contacts by name in multiple directories simultaneously. The new **All** menu item in the **Directories** menu provides this function. The phone searches for the name in the following locations if Broadsoft directories are configured:

- All Broadsoft directories
    - Enterprise directory
    - Group directory (included in the Enterprise directory)
    - Enterprise Common directory
    - Group Common directory
    - Personal directory

- The LDAP directory, if configured
- The personal address book on the phone
- Bluetooth-synchronized contacts

The search function behaves in a similar manner to the name-search function within individual directories. The search results show both full and partial name matches. You can select a contact in the search results and then view contact details, add the contact to the personal address book, and call the contact. You can also edit the number before making the call.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Voice Feedback

The Voice Feedback feature is available on the Cisco IP Phone 8800 Series Multiplatform Phones. This feature enables visually impaired and blind persons to work effectively with the Cisco phones. The phone's voice feedback reads incoming caller IDs, displayed screens and settings, and button functions.

This feature makes softkeys easy to identify and use.

- Press a softkey once, and the voice reads the feature that is associated with the key.
- Press the softkey twice, and the feature is executed.

Voice Feedback is enabled and disabled with the **Select** button that is located in the center of the Navigation cluster. Press the **Select** button three times quickly to turn the Voice Feedback On, and three times again to turn it Off. The phone's audible feedback reads the screen name followed by the application or setting that is highlighted on the screen.

By default, the Voice Feedback feature uses your speakerphone to alert you. However, if you lift the handset from the cradle, or use a headset, the audible feedback will be heard through the handset or headset, instead.

You may not hear Voice Feedback if you select the Headset button, but don't have a connected headset. Select **Speakerphone** and you hear Voice Feedback again.

The Voice Feedback feature is available only for English language users.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Wi-Fi Feature Enhancements

You and your user can set up maximum of four Wi-Fi profiles from the phone web page, the phone menu, the XML provisioning server, and the TR69 ACS server. The phone then uses this list of profiles to connect to a Wi-Fi automatically or manually when you turn on the phone Wi-Fi. The profile that appears at the top of the list has the highest priority and the phone connects automatically to a Wi-Fi using this profile while provisioning. You can also connect to a Wi-Fi manually, by scanning available Wi-Fi profiles, and then providing details of that selected profile.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Upgrade the Firmware

You can upgrade the phone firmware with TFTP, HTTP, or HTTPS. After the upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click this link:

https://software.cisco.com/download/home/286311392

On the **Software Download** web page that is displayed, ensure that **IP Phone 8800 Series with Multiplatform Firmware** is selected in the middle pane.

Step 2 Select your phone model in the right pane.

Step 3 On the next page that is displayed, select **Multiplatform Firmware**.

Step 4 On the next page that is displayed, select **11.2.3** in the **All Releases** > **MPPv11** folder.

Step 5 (Optional) Place your mouse pointer on the file name to see the file details and checksum values.

Step 6 Download the firmware `cmterm-88xx.11-2-3MPP-nnn_REL.zip` file:

- For Cisco IP Phone 8811, 8841, 8851, and 8861 Multiplatform Phones:
  `cmterm-88xx.11-2-3MPP-398_REL.zip`
- For Cisco IP Phone 8845 and 8865 Multiplatform Phones:
  `cmterm-8845_65.11-2-3MPP-398_REL.zip`

Step 7 Click **Accept License Agreement**.

Step 8 Unzip the file and place the files in the appropriate location on your upgrade server.

The appropriate location is the TFTP, HTTP, or HTTPS download folder, depending on the protocol that you want to use for the upgrade.

Step 9 Upgrade the phone firmware with one of these methods.

- Upgrade the phone firmware from the phone administration web page:
  1. On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Provisioning** > **Firmware Upgrade**.
  2. In the **Upgrade Rule** field, enter the load file URL as described below.

     Load file URL format:

     ```
     <upgrade protocol>://<upgrade server ip
     address>[:<port>]>/<path>/<file name>.loads
     ```

     Example:

```
https://10.73.10.223/firmware/sip88xx.11-2-3MPP-398.loads
```

3. Click **Submit All Changes**.

- Upgrade the phone firmware directly from your web browser:

  In the address bar of your web browser, enter the phone upgrade URL as described below.

  Phone upgrade URL format:

  ```
  <phone protocol>://<phone ip address[:port]>/admin/upgrade?<load file URL>
  ```

  Load file URL format:

  ```
  <upgrade protocol>://<upgrade server ip address>[:<port>]>/<path>/<file name>.loads
  ```

  Example:

  ```
  https://10.74.10.225/admin/upgrade?https://10.73.10.223/firmware/sip88xx.11-2-3MPP-398.loads
  ```

Note Specify the `<file name>.loads` file in the URL. The `<file name>.zip` file contains other files.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Caveats

View Caveats

You can search for caveats (bugs) with the Cisco Bug Search tool.

Known caveats are graded according to severity level, and are either open or resolved.

Before you begin

You have your Cisco.com user ID and password.

Procedure

Step 1 Click one of the following links:

- To view all caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(3)&sb=anfr&bt=custV

- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(3)&sb=anfr&sts=open&bt=custV
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(3)&sb=anfr&sts=fd&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) For information about a specific caveat, enter the bug ID number (*CSCxxnnnnn*) in the **Search for** field, and press **Enter**.

Open Caveats

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco IP Phone 8800 Series Multiplatform Phones that use Firmware Release 11.2(3).

This list reflects a snapshot of the caveats that were open at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the open caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 10. You must be a registered Cisco.com user to access this information.

- CSCvn71980 Can't re-connect to mobile phone after try to connect other device
- CSCvn97024 Add new softkey come out after search result refresh eventhough contact book full
- CSCvn99652 Microphone not translated correctly in HK locale

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Phone 8800 Series Multiplatform Phones that use Firmware Release 11.2(3).

This list reflects a snapshot of the caveats that were resolved at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the resolved caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 10. You must be a registered Cisco.com user to access this information.

- CSCvm04387 494 Security Agreement Required: Error not handled
- CSCvm18798 No Way Audio resuming a call on hold over 5min
- CSCvm42595 Crash After Basic Call - SRTP
- CSCvm55043 MPP phones - 'PUBLISH' failsover randomly drops call setup over TLS
- CSCvm69980 Device is continuously ringing
- CSCvn00136 Phones Dropping Calls When Caller ID is the Same
- CSCvk61693 Device is crashing and rebooting
- CSCvm08412 Phone crash when make an outgoing call
- CSCvm18798 No Way Audio resuming a call on hold over 5min

- CSCvm24436 Evaluation of MPP-88xx for CVE-2018-5391 (FragmentSmack)
- CSCvm25595 UI not responding while generating PRT
- CSCvn05579 PRT does not include archive
- CSCvn33390 LDAP: search entry is wrong, phone unable to get contact's telephone number and other information
- CSCvn64431 Phone crash after press option if the cursor in leftmost when search person address book
- CSCvn78102 Can't change volume when use bluetooth headset as audio path
- CSCvm14205 Cannot Enable Call Recording w/ SIP REC: INVITE SDP Does not Include XML Metadata
- CSCvn64085 No Video During Point to Point Calls
- CSCvn99848 Phone reboot when press hold button

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see https://cisco.com/go/phonefirmwaresupport.

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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 of this document are considered uncontrolled. See the current online version for the latest version.

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

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. (1721R)