Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 11.2(1)

First Published: 2018-07-30

Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 11.2(1)

Use these release notes with the following Cisco IP Phone 8800 Series Multiplatform Phones running SIP Firmware Release 11.2(1).

- 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

BroadWorks Anywhere

You can configure a phone to allow a call to seamlessly move from one desk phone or location to another mobile phone or desk phone or location. The user can receive an incoming call from multiple locations. When you enable this feature, the user can edit the locations list from the **Anywhere** menu on the phone screen.

You can enable this feature on the phone web page from **Voice** > **Ext (n)** > **XSI Line Service**.

Where to Find More Information

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

BroadWorks XSI Call Logs Display

You can enable the user to view local call logs or remote call logs recorded at the XSI server. When you enable the feature, the user sees the **Display recents from** menu in the **Recents** list of the phone.

You can configure this feature on the phone web page from **Voice** > **Phone** > **XSI Phone Service**.

Where to Find More Information

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

Bypass the Set Password Screen

As a service provider, you can enable users to bypass the **Set password** screen on the first boot or after a factory reset.

The phone attempts to configure itself using DHCP or EDOS settings that can include a user password. The phone software waits until the DHCP configuration completes and the EDOS configuration attempt completes, before it reads the phone configuration file. If you set a user password in the phone configuration file, the **Set password** screen does not display.

Where to Find More Information

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

BroadWorks XSI Caller ID Blocking

You can block the display of a phone's caller ID from the phone screen. When you enable this feature, the caller ID does not display on the called phone when the user makes an outgoing call.

When you enable this feature, the **Block caller id** menu is displayed on the phone screen. This menu allows the user to block the phone's caller ID.

You can enable this feature on the phone web page from **Voice** > **Ext(n)** > **XSI Line Service**.

Where to Find More Information

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

EDOS Certificate and Encryption Enhancements

As a service provider, you can upload your root Certificate Authority (CA) file to the Cisco EDOS server. The formats supported are: .pem, .cer, .cert, .crt.

When you upload your root certificate file to EDOS, the server provides a URL to the certificate. You use the URL as the Custom CA URL when you configure devices.

As well, you can also select the encryption hash (MD5, SHA1, or SHA256) when Cisco signs your CSR. Cisco recommends that you select SHA256, which provides the highest security.

Where to Find More Information

- Cisco EDOS documentation and online help
- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Executives and Assistants

You can set up executives and their assistants to share control of calls.

You configure users as executives and assistants in BroadWorks. The BroadWorks configuration also sets up the relationships between the executives and assistants. For more information, see the BroadWorks documentation.

After the BroadWorks configuration, you configure the phone settings.

When configuration is complete, executives and assistants can share control of the executives' calls, on their own respective phones. Assistants can answer and initiate calls on behalf of executives, and transfer ongoing calls to executives. Executives can join calls or transfer calls to themselves. Assistants can divert their incoming executives' calls to another number when necessary.

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*

Incoming Call Silence

You can configure an **Ignore** softkey on the phone that the user can press to silence an incoming call. The user presses the **Ignore** softkey or the Volume down button to silence the incoming call.

You can configure the softkey in the **Programmable Softkeys** area from **Voice** > **Phone** on the phone web page.

Where to Find More Information

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

NAPTR Support

You use the Name Authority Pointer (NAPTR) to allow the phone to automatically determine and select the appropriate transport protocol for the phone line.

As before, you can specify the transport protocol of your choice (UDP, TCP, or TLS) on the phone web page. You use the new Auto option in the SIP transport field to enable the phone to automatically select the protocol.

You can configure the setting in the **SIP Transport** field from **Voice** > **Ext(n)** > **SIP Settings** on the phone web page.

When you configure the setting to Auto, the phone determines the transport protocol based on the Name Authority Pointer (NAPTR) records on the DNS server. The phone uses the protocol specified in the record that has the lowest order and preference. When there are multiple records with the same order and preference, the phone looks for a protocol within the records, in the following order of preference: UDP, TCP, and TLS. The phone uses the highest priority protocol that it finds in a record.

Where to Find More Information

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

New Domain Support while Provisioning

When a phone connects to a network for the first time or after a factory reset, if there are no DHCP options setup, it contacts a device activation server for zero touch provisioning. Starting with this firmware release, phones will use activate.cisco.com instead of webapps.cisco.com for provisioning. Phones with older versions of the firmware will continue to use webapps.cisco.com. Cisco recommends that you allow both the domain names through your firewall.

Where to Find More Information

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

Peer Firmware Sharing

You can enable Peer Firmware Sharing (PFS) when you want a phone to find other phones of the same model or series on the subnet and share updated firmware files. The phones are organized into a hierarchy using Cisco Peer-to-Peer-Distribution Protocol (CPPDP), which is a Cisco proprietary protocol. One of the phones in that hierarchy acts as a root phone. The root phone downloads the firmware image from the load server and then transfers the firmware to other phones in the hierarchy.

You can configure this feature on the phone web page from **Voice** > **Provisioning** > **Firmware Upgrade**.

Where to Find More Information

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

Phone Menu Access Control

You can restrict the access to the phone menus and options on the phone screen by configuring the provisioning file. The configurations take effect when the parameter Phone-UI-User-Mode (in the **Voice** > **System** > **System Configuration** section) is Yes.

- When an element is designated with ua="na", users don't see the Settings menu on the phone screen.
- When an element is designated with ua="ro", users can see the Settings menu on the phone screen, but can't change the settings.
- When an element is designated with ua="rw", users can see the Settings menu and change the settings on the phone screen.

Where to Find More Information

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

Priorities for Voice and Video Data

You can now prioritize voice or video data in limited bandwidth conditions.

You will need to configure the priorities individually on each line of a phone.

You can configure different priorities for different areas of traffic. For example, you can configure different priorities for internal and external traffic by configuring one set of priorities on internal lines and another set of priorities on external lines. For effective traffic management, specify the same settings on all the phone lines in a group.

The Type of Service (ToS) field of a data packet determines the packet's priority in data traffic. You can configure the desired priorities by specifying appropriate values for the ToS fields of voice and video packets, for each phone line.

You can set up these values on the phone web page.

For voice data, there is no change in behavior. The phone applies the ToS value that it receives by LLDP. When there is no ToS value available by LLDP, the phone applies the value that you have specified for voice packets.

For video data, the phone always applies the ToS value that you have specified for video packets.

The default values prioritize voice over video.

Where to Find More Information

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

Privacy Header Configuration

Privacy header configuration protects user privacy. You can specify the level of user privacy within your trust network. The levels available are: Disabled (default), none, header, session, user, and id.

You use the administration phone web page or add XML tags to the **`config.xml`** provisioning file. You can set each of the 10 phone line extensions to send out a specific privacy header and request user privacy needs in the SIP messages.

You can configure the privacy header on the phone web page from **Voice** > **Ext(n)** > **SIP Settings**.

Where to Find More Information

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

Profile Account for 401 HTTP Authentication Error

Users can now quickly and easily collect authentication information used for provisioning when the phone receives HTTP or HTTPS 401 authentication response. When this error occurs, the **Profile Accounts Setup** screen is displayed on the phone, and users can collect their user ID and password for the phone to resynchronize.

You can enable this feature in the **Configuration Profile** area from **Voice** > **Provisioning** on the phone web page.

Where to Find More Information

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

Ringtone Menu Change

Your user can access the **Ringtone** menu under the **User preferences** screen to change the ringtones of the phone.

Where to Find More Information

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

Screen Saver Type without Lock Option

You can only add three types of screen saver: **Clock**, **Logo**, and **Download Picture**. Support for “lock” as one of the screen saver type is removed now.

If the user configures screen saver type to lock with TR069 and config file, the screen saver type default is set to **Clock**.

Where to Find More Information

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

SIP Message Blocking from a Non-Proxy Device

The phone can now silently block or ignore any Session Initiation Protocol (SIP) messages from a non-proxy device. When the phone discards such messages, the user does not see any notifications on the phone screen. You can enable or disable this feature by changing the values in the **Block Nonproxy SIP** field from the phone web page or from xml provisioning.

Set **Block Nonproxy SIP** to No for phones that use TCP or TLS to transport SIP messages. Nonproxy SIP messages transported over TCP or TLS are blocked by default.

When non-proxy messages are blocked, the phone only accepts SIP messages from:

- proxy server
- outbound proxy server
- alternative proxy server
- alternative outbound proxy server
- IN-Dialog message from both proxy and non-proxy device. For example, Call session dialog and Subscribe dialog.

Where to Find More Information

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

TR-069 Provisioning Enhancements

If you use TR-069 to configure the phones, the list of parameters available is extended. This feature ensures that you can manage phone devices in your network with Auto Configuration Server (ACS), instead of an XML provisioning server.

Where to Find More Information

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

Video Packetization Mode 1 Support

The Cisco IP Phone 8845 and 8865 support the H.264 High Profile packetization mode 1, Base Profile packetization mode 0, and Base Profile packetization mode 1.

This feature requires no configuration.

Where to Find More Information

Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide

Upgrade the Firmware

The *Cisco IP Phone 8800 Series Multiplatform Phones* support two firmware image upgrades that use TFTP, HTTP, or HTTPS.

- Cisco IP Phone 8811, 8841, 8851, and 8861 with Multiplatform Firmware (Audio only)
- Cisco IP Phone 8845 and 8865 with Multiplatform Firmware (Video)

After the firmware upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click the following URL:

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

Step 2 Select **IP Phone 8800 Series with Multiplatform Firmware** in the middle pane.

Step 3 Select your phone model (with Multiplatform Firmware) in the right pane.

Step 4 Select the **Multiplatform Firmware** software type.

Step 5 In the **All Releases** > **MPPv11** folder, select **11.2.1**.

Step 6 (Optional) Place your mouse pointer on the filename to display the file details and checksum values.

Step 7 Download one of these files:

- For the 8811, 8841, 8851, and 8861 `cmterm-88xx.11-2-1MPP-630_REL.zip`
- For the 8845 and 8865 `cmterm-8845_65.11-2-1MPP-630_REL.zip`

Step 8 Click **Accept License Agreement** when you accept the software license.

Step 9 Unzip the firmware files.

Step 10 Put the files in the TFTP, HTTP, or HTTPS download directory.

Step 11 You can upgrade the phone firmware using either of the following methods:

- Configure the **Upgrade Rule** on the **Provisioning** tab in the phone web page with the upgrade URL.

  URL Format: <upgrade_protocol>://<serv_ip[:port]>/<filepath>/sipMMxx.RR-nnn.loads

  Where the user input values are:

  - **`<upgrade_protocol>`**–HTTP, TFTP, or HTTPS.
  - **`<serv_ip[:port]>`**–Server IP address and optional port number.
  - **`<filepath>`**–File folder on the server that contains the firmware upgrade `*.loads` file.
  - **`MMxx`**–Cisco IP Phone MM Series with Multiplatform Firmware (for example, 68xx, 78xx, or 88xx)

    or

    `MMxx`–Cisco specific phone model (for example, 8845_65 or 8861)
  - **`RR`**–Major and minor release numbers (for example, 11-2-1 or 11-1-1SR1)
  - **`nnn`**–Build number (for example, 351)

  Example using the **Upgrade Rule** for the Cisco IP 8811, 8841, 8851, and 8861 phones.

  `tftp://10.73.10.192/firmware/sip88xx.11-2-1MPP-630.loads`

- Provide a URL in a web browser that directs the call server to download the firmware to the phone.

  URL Format: <phone_protocol>://<phone_ip[:port]>/admin/upgrade?

  <upgrade_protocol>://<serv_ip[:port]>/<filepath>/sipMMxx.RR-nnn.loads

  Where the user input values are:

  - **`<phone_protocol>`**–HTTP or HTTPS only.
  - **`<phone_ip[:port]`**–Phone IP address and optional port number.
  - **`<upgrade_protocol>`**–HTTP, TFTP, or HTTPS.
  - **`<serv_ip[:port]>`**–Server IP address and optional port number.
  - **`<filepath>`**–File folder on the server that contains the firmware upgrade `*.loads` file.
  - **`MMxx`**–Cisco IP Phone MM Series with Multiplatform Firmware (for example, 68xx, 78xx, or 88xx)

    or

    `MMxx`–Cisco specific phone model (for example, 8845_65 or 8861)
  - **`RR`**–Major and minor release numbers (for example, 11-2-1 or 11-1-1SR1)
  - **`nnn`**–Build number (for example, 351)

Example using the **web browser URL** for the Cisco IP 8845 and 8865 phones.

```
https://10.74.10.225/admin/upgrade?http//10.73.10.192/firmware/sip8845_65.11-2-1MPP-630.loads
```

Note Use the `*.loads` file in the URL. The `*.zip` file contains other files.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- 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 using the Cisco Bug Search tool.

Known caveats (bugs) are graded according to severity level, and can be either open or resolved.

Before you begin

To view the caveats, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Step 1 Perform one of the following actions:

- To find all of the caveats for the 11.2.1 release, use this URL: https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(1)&sb=anfr&bt=custV
- To find all open caveats for the 11.2.1 release, use this URL: https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(1)&sb=afr&sts=open&bt=custV
- To find all resolved caveats for the 11.2.1 release, use this URL: https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.2(1)&sb=afr&sts=fd&bt=custV

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

Step 3 (Optional) To look for information about a specific problem, 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(1).

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier (*CSCxxnnnnn*). You must be a registered Cisco.com user to access this defect information.

Because the defect status continually changes, the list reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of the open defects or to view specific bugs, access the Bug Search Toolkit as described in the View Caveats, on page 9.

Note Some caveats only apply to specific Cisco IP Phone 8800 Series with Multiplatform Firmware phones. The list annotates these caveats using this example notation: **[8845 and 8865 only]**.

- CSCvi51486 Vulnerable Linux kernel version in use
- CSCvi99280 Phone will switch between more than one server time after rebooting when the phone is set to IPv6 only and uses IPv6 address.
- CSCvk17587 Phone can not scan the SSID connected last time any more when the 2.4GHz band on WLC is disabled.
- CSCvk17748 KEM background still lights up when the phone lost the Wi-Fi connection.
- CSCvk30143 Wi-Fi: After DHCP address release, network connection status will be abnormal.
- CSCvk31532 Use DNS from DHCP when DNS Server Order is Manual only
- CSCvi72223 : 8845:resync use “autoconfig IPv6 IP address” and not “DHCP IPv6 IP address”
- CSCvk21379 Phone reboots repeatedly when registered through Wi-Fi with 5.0GHz mode.
- CSCvk37625 Key system: Sometimes two entries pop up when receiving an incoming call for DUT
- CSCvk43167 Anonymous shows on phone screen on non-shared line where two shared lines are configured at the same time.
- CSCvk22456 JPN: Message “Failed to get XSI settings. DNS error” on phone screen is not localized.

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(1).

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier (*CSCxxnnnnn*). Register at Cisco.com to access this defect information.

Because the defect status continually changes, the list reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of the resolved defects or to view specific bugs, access the Bug Search Toolkit as described in the View Caveats, on page 9.

Note Some caveats only apply to specific Cisco IP Phone 8800 Series with Multiplatform Firmware phones. The list annotates these caveats using this notation: **[8845 and 8865 only]**.

- CSCvc65877 "BLF+Speed Dial" setting makes *status.xml* not accessible and Call status messed up
- CSCvc90927 Incorrect translation for German (Phone shows VERWENDET, which means USED and not BUSY)
- CSCvb84547 Phone resets upon change of PC port status
- CSCvb86426 After dialing only 2 digits, phone goes onhook
- CSCvc94312 PSK definition with quotation (") substitution failing to display name
- CSCvc96190 BLFs blink off then back on periodically
- CSCvc96607 Call transfer fails
- CSCvb93247 NAT Keep Alive Message always sends SIP Notify
- CSCvb95670 Programmable Softkeys do not work correctly on an active call
- CSCvc27587 User_Agent $VERSION does not work
- CSCvc27602 BLF subscribe, illegal Cseq numbers from CP-7861
- CSCvc27606 Slow User Interface
- CSCvc27608 Call fails when the called phone puts the call on hold
- CSCvc29353 Cisco IP Phone 8800 Series SIP Denial of Service Vulnerability
- CSCvc30728 Phone deregisters when "Auto Vlan" is selected
- CSCvc30743 IT NAT keep alive not working in MPP
- CSCvc97835 Authenticated SIP Notify for Prov Refresh failing
- CSCve78758 Phone is continuously ringing after call park
- CSCvf04597 Phone ID is not set in CDP
- CSCvf06312 DUT phone can't hear the remote party for 1-2 seconds
- CSCvf62629 Phone parsing error after receiving SIP message with big "Record-Route" entries
- CSCvf77452 When provisioning a secondary configuration file to 8861 phone, Resource Exhausted error message appeared
- CSCvf77534 SIP Line failing to perform SIP REG FAILOVER to secondary SBC
- CSCvf86343 Line ID Mapping not working for incoming calls
- CSCvf96271 Phone continuously reboots after adding more than 100 contacts via provisioning

- CSCvf96764 BLF unsubscribed at 1800 seconds after receiving blank dialog NOTIFY
- CSCvf96974 8861 phone fails to obtain IP address after reboot when on Voice VLAN
- CSCvg03527 Resumed call does not use offhook handset, but Preferred Audio Device
- CSCvg15839 BXfer On Speed Dial incorrectly initiates a new call during an active call when dialing to its own extension
- CSCvg18498 Maximum length of Speed-dial button is too short
- CSCvg29271 Phone answers to unsolicited SIP messages even after setting “Restricted Access Domains”
- CSCvg29326 Voice Quality Report not getting set
- CSCvg38265 Key reinstallation attacks against WPA protocol
- CSCvg40114 Emergency Call is failing to block hold/endCall user actions
- CSCvg41339 88xx-MPP: Inconsistent handling of InfoSec trusted CA
- CSCvg42488 BLF incorrectly shows as available when monitored line is in use
- CSCvg57045 Missing value of “User=Phone” tag caused transfer/conference issues
- CSCvg67251 NWay Conference Reject not handled gracefully
- CSCvg77605 Phone sends an unwanted PUBLISH right after an outgoing to PSTN is established
- CSCvg87084 Calls from MPP phone to VoLTE registered devices fail
- CSCvh16184 Under Certain Circumstances, phone does not accept configuration of TIME_FORMAT
- CSCvh44179 When 3rd phone put the crypo which MPP can recognize after 5th, MPP SDP negotiation will fail.
- CSCvh48979 Agent's ACD state remains in an "Available" State permanently
- CSCvh61930 Phone becomes slow and eventually freezes
- CSCvh62303 Issue upgrading - missing host header on HTTP upgrade
- CSCvi26086 No audible tone when using paging service
- CSCvi29841 PRT upload showing Error for 20x responses
- CSCvi32423 SIP stack mishandling Tel URL
- CSCvi51426 Cisco Phone web page command injection vulnerability
- CSCvi68771 Device cannot dial ## when locale CW is activated
- CSCvg66758 XML configuration for phone background not backward-compatible
- CSCvg75487 Video phone parses dictionary server error
- CSCvh73357 **[8845 and 8865 only]** Phone does not always display video

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.