Troubleshooting and Maintenance

- Troubleshooting and Maintenance Overview, on page 1
- Troubleshooting, on page 1
- Maintenance, on page 22

Troubleshooting and Maintenance Overview

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. It also explains how to clean and maintain your phone.

For additional troubleshooting information, see the *Using the 79xx Status Information For Troubleshooting* tech note. This document is available to registered Cisco.com users at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_tech_note09186a00800945bd.shtml

Troubleshooting

This section includes the following topics:

Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in Phone Startup Process. If the phone does not start up properly, see the following sections for troubleshooting information:

Cisco Unified IP Phone Does Not Go Through Normal Startup Process

Problem

When you connect a Cisco Unified IP Phone into the network port, the phone should go through the normal startup process, and the LCD screen should display information.

Cause

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, or lack of power. Or, the phone may not be functional.

Solution

To determine whether the phone is faulty, follow these suggestions to systematically eliminate these other potential problems:

1. Verify that the network port is functional:
   - Exchange the Ethernet cables with cables that you know are functional.
   - Connect a operational phone to this network port to verify the port is active.
   - Replace an operational phone with the nonoperational phone.
   - Connect the nonoperational phone directly to the port on the switch, eliminating the patch panel connection in the office.
2. Verify that the phone is receiving power:
   - If you are using external power, verify that the electrical outlet is functional.
   - If you are using in-line power, plug the phone into an electrical outlet using the external power supply.
   - If you are using the external power supply, switch the power supply with a unit that you know works.
   - Make sure that the phone is connected to a switch that supports IEEE 802.3af Class 3 (15.4 W in-line power at the switch port).
3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
4. If the phone still does not start up properly, perform a factory reset of the phone.

If after attempting these solutions, the LCD screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Related Topics

Phone Startup Process
Cisco Unified IP Phone Power
Factory Reset, on page 20

Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the LCD screen, the phone is not starting up properly. The phone cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason the phone is unable to start up properly:

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See Status Messages Screen for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

Problem

If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

Solution

Ensure that the network is currently running.

TFTP Server Settings

Problem

The TFTP server settings may not be correct.

Solution

Check the TFTP settings. See Check TFTP Settings, on page 13.

IP Addressing and Routing

Problem

The IP addressing and routing fields may not be correctly configured.

Solution

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually. See Check DHCP settings, on page 13.

DNS Settings

Problem

The DNS settings may be incorrect.

Solution

If you are using DNS to refer to the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. See Verify DNS Settings, on page 14.

Cisco Unified Communications Manager Settings on Phone

Problem

The phone may have the wrong Cisco Unified Communications Manager information.

Solution

On the Cisco Unified IP Phone, press the **Settings** button, choose **Device Configuration**, and look at the Unified CM Configuration options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified Communications Manager. See Cisco Unified Communications Manager Phone Registration, on page 4 for tips on resolving this problem.

Cisco CallManager and TFTP Services Are Not Running

Problem

If the Cisco CallManager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a systemwide failure, and other phones and devices are unable to start up properly.

Solution

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 15.

Configuration File Corruption

Problem

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Solution

Create a new phone configuration file. See Create New Phone Configuration File, on page 14.

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with Cisco Unified Communications Manager.

Solution

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if autoregistration is enabled. Review the information and procedures in Cisco Unified Communications Manager Phone Addition Methods to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** > **Find** from Cisco Unified Communications Manager Administration to search for the phone based on the MAC Address. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Configuration File Corruption, on page 4 for assistance.

Cisco Unified IP Phone Cannot Obtain IP Address

Problem

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

Cisco Unified IP Phone Displays Security Error Message

Problem

The phone displays “Security Error” on the screen.

Cause

When a Cisco Unified IP Phone boots, it performs an internal Power On Self Test (POST). POST checks for existing encryption functionality. If POST detects that encryption functionality is missing, the phone fails to boot, and the message “Security Error” appears on the screen.

Solution

To correct the problem, perform the following steps:

1. Reset the phone manually.
2. If the phone does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
3. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see Factory Reset, on page 20.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

Physical Connection Problems

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco Unified IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Intermittent Network Outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

The following suggestions can help you determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. For more information, see Network Configuration Menu.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

   Cisco Unified IP Phone 7971G-GE and 7970G send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease will be denied, forcing the Cisco Unified IP Phone 7971G-GE and 7970G to restart and request a new IP address from the DHCP server.

Static IP Address Setting Errors

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone has been assigned a static IP address, verify that you have entered the correct settings.

Voice VLAN Setup Errors

Problem

If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to same switch as phone), it is likely that you do not have a voice VLAN configured.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phones Have Not Been Intentionally Reset

Problem

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

Solution

You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Applications Menu** button on the phone and choosing **Settings** > **Status** > **Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset: Phone received a Reset-Reset request from Cisco Unified Communications Manager Administration.
- Reset-Restart: Phone received a Reset-Restart request from Cisco Unified Communications Manager Administration.

DNS or Other Connectivity Errors

Problem

The phone reset continues and you suspect DNS or other connectivity issues.

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors with Determine DNS or Connectivity Issues, on page 15.

Power Connection Problems

Problem

The phone does not appear to be powered up.

Solution

In most cases, a phone restarts if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then connects to an external power supply.

Cisco Unified IP Phone Security Problems

The following sections provide troubleshooting information for the security features on the Cisco Unified IP Phone. For information about the solutions for any of these issues, and for additional troubleshooting information about security, see *Cisco Unified Communications Manager Security Guide*.

CTL File Problems

The following sections assist in troubleshooting CTL file problems.

Authentication Error, Phone Cannot Authenticate CTL File

Problem

A device authentication error occurs.

Cause

CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.

Solution

Install a correct certificate.

Phone Cannot Authenticate CTL File

Problem

Phone cannot authenticate the CTL file.

Cause

The security token that signed the updated CTL file does not exist in the CTL file on the phone.

Solution

Change the security token in the CTL file and install the new file on the phone.

ITL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the ITL file.

Cause

The configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Re-sign the configuration file by using the correct certificate.

Phone Does Not Register

Problem

Phone does not register with Cisco Unified Communications Manager.

Cause

The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.

Solution

Change the Cisco Unified Communications Manager server information in the CTL file.

Signed Configuration Files Are Not Requested

Problem

Phone does not request signed configuration files.

Cause

The CTL file does not contain any TFTP entries with certificates.

Solution

Configure TFTP entries with certificates in the CTL file.

802.1X Authentication Problems

802.1X authentication problems can be broken into the categories described in the following table.

Table 1: Identifying 802.1X Authentication Problems

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays as “Configuring IP” or “Registering.” • 802.1X Authentication Status displays as “Held” (see 802.1X Authentication and Status Menus for more details). • Status menu displays 802.1X status as “Failed” (see Status Menu for more details).	802.1X Enabled on Phone but Phone Does Not Authenticate, on page 10

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address • Phone does not register with Cisco Unified Communications Manager • Phone status display as “Configuring IP” or “Registering” • 802.1X Authentication Status displays as “Disabled” • Status menu displays DHCP status as timing out	802.1X Not Enabled, on page 10
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status display as “Configuring IP” or “Registering.” • Cannot access phone menus to verify 802.1X status.	Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 11

802.1X Enabled on Phone but Phone Does Not Authenticate

Problem

The phone cannot authenticate.

Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

1. Verify that you have properly configured the required components (see 802.1X Authentication for more information).
2. Confirm that the shared secret is configured on the phone (see 802.1X Authentication and Status Menus for more information).
   - If the shared secret is configured, verify that you have the same shared secret entered on the authentication server.
   - If the shared secret is not configured, enter it, and ensure that it matches the one on the authentication server.

802.1X Not Enabled

Problem

The phone does not have 802.1X configured.

Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution

To enable it, see 802.1X Authentication and Status Menus.

Factory Reset of Phone Has Deleted 802.1X Shared Secret

Problem

After a reset, the phone does not authenticate.

Cause

These errors typically indicate that the phone has completed a factory reset (see Factory Reset, on page 20) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

Solution

To resolve this, you have two options:

- Temporarily disable 802.1X authentication on the switch.
- Temporarily move the phone to a network environment that is not using 802.1X authentication.

Once the phone starts up normally in one of these conditions, you can access the 802.1X configuration menus and re-enter the shared secret (see 802.1X Authentication and Status Menus).

Audio and Video Problems

The following sections describe how to resolve audio and video problems.

Phone Display Is Wavy

Problem

The display appears to have rolling lines or a wavy pattern.

Cause

The phone might be interacting with certain types of older fluorescent lights in the building.

Solution

Move the phone away from the lights or replace the lights to resolve the problem.

No Speech Path

Problem

One or more people on a call do not hear any audio.

Solution

When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

General Telephone Call Problems

This section describes troubleshooting of general telephone call problems.

VPN-Connected Phone Does Not Log Calls

Problem

A remote location (home office) phone that is connected through the VPN does not log missed, placed, or received calls.

Cause

Without explicitly setting the Alternate TFTP setting, the Cisco IP Phone cannot contact the TFTP server and download the configuration and other files, and function properly.

Solution

Set up the phone to use the Alternate TFTP server and configure the TFTP server IP address.

Related Topics

Set Up Remote Phone, on page 12

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Set Up Remote Phone

Cisco IP Phones that are configured for SSL VPN to ASA using the built-in client in a remote location (for example, a home office) have a special configuration requirement.

We recommend that you provide the phone with an Alternate TFTP server setting manually. This setting allows the phone to download the configuration and other files from TFTP. The phone in a remote location (home office) cannot correctly provide OPTION 150 to the phone using DHCP.

The IP phone can register to the last-known Cisco Unified Communications Manager, but any configuration updates cannot applied until you configure the manual TFTP server address.

Procedure

Step 1 On the phone, select **Applications**.

Step 2 Navigate to the **IPv4 Settings** window.

Step 3 Scroll to the Alternate TFTP option and set the field to **Yes**.

Step 4 In the TFTP Server 1 field, set the TFTP server address.

Step 5 Save the changes.

Check TFTP Settings

Procedure

Step 1 You can determine the IP address of the TFTP server used by the phone by pressing the **Settings** button on the phone, choosing **Network Configuration** > **IPv4**, and scrolling to the **TFTP Server 1** option.

Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See Network Configuration Menu.

Step 3 If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.

Step 4 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See Network Configuration Menu for instructions.

Check DHCP settings

Procedure

Step 1 On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the following options:

- DHCP Server: If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. See *Troubleshooting Switch Port Problems* at this URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_tech_notes_list.html
- IP Address, Subnet Mask, Default Router: If you have assigned a static IP address to the phone, you must manually enter settings for these options. See Network Configuration Menu for instructions.

Step 2 If you are using DHCP, check the IP addresses distributed by your DHCP server. See *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* at this URL: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Verify DNS Settings

To verify DNS settings, perform these steps.

Procedure

Step 1 Verify this setting by pressing **Settings**.

Step 2 Choose **Network Configuration** and scroll to the **DNS Server 1** option.

Step 3 Verify that a CNAME entry exists in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

Step 4 Ensure that DNS is configured to do reverse look-ups.

Create New Phone Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Note

- When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DNs" and can be used for other devices. If unassigned DNs are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

To create a new configuration file, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device** > **Phone** > **Find** to locate the phone experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Step 3 Add the phone back to the Cisco Unified Communications Manager database. See Cisco Unified Communications Manager Phone Addition Methods for details.

Step 4 Power cycle the phone.

Start Service

Note A service must be activated before it can be started or stopped. To activate a service, choose **Tools** > **Service Activation**.

To start a service, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2 Choose **Tools** > **Control Center - Feature Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

Step 4 If a service has stopped, click the corresponding radio button and then click **Start**.

The Service Status symbol changes from a square to an arrow.

Determine DNS or Connectivity Issues

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

Step 1 Use the **Erase** softkey to reset phone settings to their default values. See Cisco Unified IP Phone Reset or Restore, on page 20 for details.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP. See Network Configuration Menu for instructions.

b) Assign static IP values to the phone. See Network Configuration Menu for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.

c) Assign TFTP server. See Network Configuration Menu for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System** > **Server** and verify that the server is referred to by the IP address and not by its DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device** > **Phone** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination.

Step 6 Power cycle the phone.

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco Unified IP Phone.

Table 2: Cisco Unified IP Phone Troubleshooting

Summary	Explanation
Daisy-chaining IP phones	Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones do not work.
Poor quality when calling mobile phones using the G.729 protocol	In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between an IP phone and a mobile phone will have poor voice quality. Use G.729 only when absolutely necessary.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.
Moving a network connection from the phone to a workstation	If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone network connection and plug the cable into a desktop computer. **Caution** The computer network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that no phone is on the line and to stop providing power to the cable.

Summary	Explanation
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Unlock and Lock Options for details.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco Unified IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service. See Call Statistics Screen for information about displaying these statistics.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. See Call Statistics Screen for information about displaying these statistics.
Gaps in voice calls	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See Call Statistics Screen for information about displaying these statistics.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to **10 Half**(10-BaseT/half duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, re-enable the port from the switch.

Summary	Explanation
Peer to peer image distribution fails.	If the peer to peer image distribution fails, the phone will default to using the TFTP server to download firmware. Access the log messages stored on the remote logging machine to help debug the peer to peer image distribution feature. **Note** These log messages are different than the log messages sent to the phone log.
Cisco VT Advantage/ Unified Video Advantage (CVTA)	If you are having problems getting CVTA to work, make sure that the PC Port is enabled, and that CDP is enabled on the PC port.
Phone call cannot be established	The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a Configuring IP or Registering message. Verify the following: **1.** The Ethernet cable is attached. **2.** The Cisco CallManager service is running on the Cisco Unified Communications Manager server. **3.** Both phones are registered to the same Cisco Unified Communications Manager. **4.** Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

Summary	Explanation
Call established with the iLBC protocol does not show that the iLBC codec is being used	Call statistics display does not show iLBC as the receiver/sender codec. 1. Check the following by using Cisco Unified Communications Manager Administration: • Both phones are in the iLBC device pool. • The iLBC device pool is configured with the iLBC region. • The iLBC region is configured with the iLBC codec. 2. Capture a sniffer trace between the phone and Cisco Unified Communications Manager and verify that SCCP messages, OpenReceiveChannel, and StationMediaTransmit messages have media payload type value equal to 86. If so, the problem is with the phone; otherwise, the problem is with the Cisco Unified Communications Manager configuration. 3. Enable audio server debug and capture logs from both phones. If needed, enable Java debug.

General Troubleshooting Tips for Cisco Unified IP Phone Expansion Module

The following table provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module.

Table 3: Cisco Unified IP Phone Expansion Module Troubleshooting

Problem	Solution
No display on the Cisco Unified IP Phone Expansion Module.	Verify that all of the cable connections are correct. Verify that you have power to the Cisco Unified IP Phone Expansion Module.
Lighted buttons on the first Cisco Unified IP Phone Expansion Module are all red.	Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.
Lighted buttons on the second Cisco Unified IP Phone Expansion Module are all amber.	Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.

Cisco Unified IP Phone Reset or Restore

Two methods exist for resetting or restoring the Cisco Unified IP Phone:

Basic Reset

Performing a basic reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these operations any time after the phone has started up. Choose the operation that is appropriate for your situation.

Table 4: Basic Reset Methods

Operation	Performing	Explanation
Restart phone	From the Main screen, press **Settings** to display the Settings menu, then press **#**. **Note** This factory reset sequence also works from any other screen that does not accept user input.	Resets any user and network configuration changes that you have made but that the phone has not written to the flash memory to previously saved settings, then restarts the phone.
Erase softkey	From the Settings menu, unlock phone options (see Unlock and Lock Options). Then press **Erase**.	Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.
	From the Network Configuration menu, unlock phone options (see Unlock and Lock Options). Then press **Erase**.	Resets network configuration settings to their default values and resets the phone. (This method causes DHCP reconfigure the IP address of the phone.)
	From the Security Configuration menu, unlock phone options (see Unlock and Lock Options). Then press the **Erase** softkey.	Deletes the CTL file from the phone and restarts the phone.

Factory Reset

When you perform a factory reset of the Cisco Unified IP Phone, the following information is erased or reset to its default value:

- CTL file: Erased
- LSC: Erased
- User configuration settings: Reset to default values
- Network configuration settings: Reset to default values

- Call histories: Erased
- Locale information: Reset to default values
- Phone application: Erased (phone recovers by loading the appropriate default load file, which depends on the phone model term75.default.loads, term71.default.loads, term70.default.loads, term65.default.loads, or term45.default.loads)

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.
- The default load file for your phone model and the files specified in that file should be available on the TFTP server that is specified by the DHCP packet.

To perform a factory reset of a phone, follow these steps:

Procedure

Step 1 Unplug the power cable from the phone and then plug it back in.

The phone begins the power-up cycle.

Step 2 While the phone is powering up, and before the Speaker button flashes on and off, press and hold **#**.

Continue to hold # until each line button flashes on and off in sequence in orange (for the Cisco Unified IP Phone 7975G, 7971G-GE and 7970G) or amber (for the Cisco Unified IP Phone 7965G and 7945G).

Step 3 Release **#** and press **123456789*0#**.

You can press a key twice in a row, but if you press the keys out of sequence, the factory reset does not take place.

After you press these keys, the line buttons on the phone flash orange and then green (for the Cisco Unified IP Phone 7975G, 7971G-GE and 7970G) or red (for the Cisco Unified IP Phone 7965G and 7945G), and the phone goes through the factory reset process. This process can take several minutes.

Do not power down the phone until it completes the factory reset process, and the main screen displays.

Additional Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, these Cisco.com websites provide you with more tips.

- Cisco Unified IP Phone Troubleshooting Resources:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- Cisco Products and Services (Technical Support and Documentation):

  http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

Maintenance

This section contains the following topics

Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified Communications Manager installation.

You can configure Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls pressing **QRT**. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses **QRT**, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information logged depends on the user selection, and if the destination device is a Cisco Unified IP Phone.

For more information about using QRT, see the *Cisco Unified Serviceability Administration Guide*.

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics based on concealment events. The Digital Signal Processor (DSP) plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics: Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics: Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.
- MOS-LQK metrics: Use a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

  MOS LQK scores are produced by a Cisco proprietary algorithm, Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores might be compliant with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.

Note Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a “human-weighted” version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see Call Statistics Screen) or remotely by using Streaming Statistics (see Remote Monitoring).

Voice Quality Metric Interpretation

To use the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss and use the metrics as a baseline for comparison.

It is important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- For Cisco Unified Phone 7975G, 7965G, and 7945G:
  - G.711 gives 4.5 score.
  - G.722 gives 4.5.
  - G.728/iLBC gives 3.9.
  - G.729A/AB gives 3.8.
- For Cisco Unified Phone 7971G-GE and 7970G:
  - G.711 codec gives 4.5 score.
  - G.729A/AB gives 3.7.

Note

- CVTQ does not support wideband (7 kHz) speech codecs, as ITU has not defined the extension of the technique to wideband. Therefore, MOS scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.
- Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality/low packet loss, and lower scores (approximately 3.5) indicate low quality/high packet loss.
- Unlike MOS, the Conceal Ratio and Concealed Seconds metrics remain valid and useful for both wideband and narrowband calls.

A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information:

Table 5: Changes to Voice Quality Metrics

Metric change	Condition
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter: • Average MOS LQK decreases could indicate widespread and uniform impairment. • Individual MOS LQK decreases indicate bursty impairment. Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.
MOS LQK scores decrease significantly	Check to see whether the phone is using a different codec than expected (RxType and TxType). Check to see whether the MOS LQK version changed after a firmware upgrade.
Conceal Ratio and Conceal Seconds increase significantly	• Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	Noise or distortion in the audio channel such as echo or audio levels. Tandem calls that undergo multiple encode/decode, such as calls to a cellular network or calling card network. Acoustic problems coming from a speakerphone, handsfree cellular phone, or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

Note Voice quality metrics do not account for noise or distortion, only frame loss.

Cisco Unified IP Phone Cleaning

To clean your Cisco Unified IP phone, use a soft, dry cloth to wipe the phone screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

Disable the screen before cleaning it so that you will not inadvertently choose a feature from the pressure of the cleaning cloth. To disable the screen, press **Display** for more than one second. The phone displays `Touchscreen Disabled` or `Phone Screen Disabled` and the **Display** button flashes green.

After one minute, the screen automatically reenables itself. To reenable the screen before that, press the flashing **Display** button for more than one second. The phone displays `Touchscreen Enabled` or `Phone Screen Enabled`.