



Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco IP Phone 7970 Series or with your IP telephony network. It also explains how to clean and maintain your phone.

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

http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html

This chapter includes these topics:

- [Resolving Startup Problems, page 9-2](#)
- [Troubleshooting Cisco IP Phone Security, page 9-12](#)
- [General Troubleshooting Tips, page 9-12](#)
- [Resetting or Restoring the Cisco IP Phone, page 9-15](#)
- [Using the Quality Report Tool, page 9-17](#)
- [Where to Go for More Troubleshooting Information, page 9-18](#)
- [Cleaning the Cisco IP Phone, page 9-18](#)

Resolving Startup Problems

After installing a Cisco IP Phone into your network and adding it to Cisco CallManager, the phone should start up as described in the “[Verifying the Phone Startup Process](#)” section on page 3-11. If the phone does not start up properly, see the following sections for troubleshooting information:

- [Symptom: The Cisco IP Phone Does Not Go Through its Normal Startup Process, page 9-2](#)
- [Symptom: The Cisco IP Phone Does Not Register with Cisco CallManager, page 9-3](#)
- [Symptom: Cisco IP Phone Resets Unexpectedly, page 9-8](#)

Symptom: The Cisco IP Phone Does Not Go Through its Normal Startup Process

When you connect a Cisco IP Phone into the network port, the phone should go through its normal startup process and the LCD screen should display information. If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, and so on. Or, the phone may not be functional.

To determine whether the phone is functional, 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.
 - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify the port is active.
 - Connect the Cisco IP Phone that will not start up to a different network port that is known to be good.
 - Connect the Cisco IP Phone that will not start up 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, use the external power supply instead.
 - If you are using the external power supply, switch with a unit that you know to be functional.
 - If you are using a Cisco IP Phone 7971G-GE, 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). For more information, see the [“Providing Power to the Cisco IP Phone 7970 Series”](#) section on [page 2-7](#).
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. For instructions, see the [“Performing a Factory Reset”](#) section on [page 9-16](#).

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

Symptom: The Cisco IP Phone Does Not Register with Cisco CallManager

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 CallManager server.

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

- [Identifying Error Messages, page 9-4](#)
- [Registering the Phone with Cisco CallManager, page 9-4](#)
- [Checking Network Connectivity, page 9-4](#)

- [Verifying TFTP Server Settings, page 9-5](#)
- [Verifying IP Addressing and Routing, page 9-5](#)
- [Verifying DNS Settings, page 9-6](#)
- [Verifying Cisco CallManager Settings, page 9-6](#)
- [Cisco CallManager and TFTP Services Are Not Running, page 9-6](#)
- [Creating a New Configuration File, page 9-7](#)

Identifying Error Messages

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 the [“Status Messages Screen” section on page 7-5](#) for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Registering the Phone with Cisco CallManager

A Cisco IP Phone can register with a Cisco CallManager server only if the phone has been added to the server or if auto-registration is enabled. Review the information and procedures in the [“Adding Phones to the Cisco CallManager Database” section on page 2-15](#) to ensure that the phone has been added to the Cisco CallManager database.

To verify that the phone is in the Cisco CallManager database, choose **Device > Find** from Cisco CallManager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see the [“Determining the MAC Address of a Cisco IP Phone” section on page 1-17](#).

If the phone is already in the Cisco CallManager database, its configuration file may be damaged. See the [“Creating a New Configuration File” section on page 9-7](#) for assistance.

Checking Network Connectivity

If the network is down between the phone and the TFTP server or Cisco CallManager, the phone cannot start up properly. Ensure that the network is currently running.

Verifying TFTP Server Settings

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**, and scrolling to the **TFTP Server 1** option.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the “[Network Configuration Menu](#)” section on page 4-6.

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. Refer to *Configuring Windows 2000 DHCP Server for Cisco CallManager*, available at this URL:

http://www.cisco.com/warp/customer/788/AVVID/win2000_dhcp.html

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 the “[Network Configuration Menu](#)” section on page 4-6 for instructions.

Verifying IP Addressing and Routing

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.

On the Cisco 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. Refer to *Troubleshooting Switch Port Problems*, available at this URL:
<http://www.cisco.com/warp/customer/473/53.shtml>
- **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 the “[Network Configuration Menu](#)” section on page 4-6 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Refer to *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, available at this URL:

<http://www.cisco.com/warp/customer/473/100.html#41>

Verifying DNS Settings

If you are using DNS to refer to the TFTP server or to Cisco CallManager, you must ensure that you have specified a DNS server. Verify this setting by pressing the **Settings** button on the phone, choosing **Network Configuration**, and scrolling to the **DNS Server 1** option. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco CallManager system.

You must also ensure that DNS is configured to do reverse look-ups. Windows2000 is configured by default only to perform forward look-ups.

Verifying Cisco CallManager Settings

On the Cisco IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the **CallManager 1–5** options. The Cisco IP Phone attempts to open a TCP connection to all the Cisco CallManager servers that are part of the assigned Cisco CallManager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco CallManager. See the “[Registering the Phone with Cisco CallManager](#)” section on page 9-4 for tips on resolving this problem.

Cisco CallManager and TFTP Services Are Not Running

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

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully.

To start a service, follow these steps:

Procedure

- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
- Step 2** Choose **Tools > Control Center**.
- Step 3** From the Servers column, choose the primary Cisco CallManager server.
The page displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.
- Step 4** If a service has stopped, click the **Start** button.
The Service Status symbol changes from a square to an arrow.
-

Creating a New 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. To create a new configuration file, follow these steps:

Procedure

- Step 1** From Cisco CallManager, choose **Device > Phone > Find** to locate the phone experiencing problems.
- Step 2** Choose **Delete** to remove the phone from the Cisco CallManager database.
- Step 3** Add the phone back to the Cisco CallManager database. See the [“Adding Phones to the Cisco CallManager Database”](#) section on page 2-15 for details.
- Step 4** Power cycle the phone.
-



Note

- When you remove a phone from the Cisco CallManager database, its configuration file is deleted from the Cisco CallManager TFTP server. The phone's directory number or numbers remain in the Cisco CallManager

database. They are called “unassigned DNSs” and can be used for other devices. If unassigned DNSs are not used by other devices, delete them from the Cisco CallManager database. You can use the Route Plan Report to view and delete unassigned reference numbers. Refer to Cisco CallManager 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 CallManager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.
-

Symptom: Cisco 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 CallManager connection are stable, a Cisco IP Phone should not reset on its own.

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

- [Verifying Physical Connection, page 9-9](#)
- [Identifying Intermittent Network Outages, page 9-9](#)
- [Verifying DHCP Settings, page 9-9](#)
- [Checking Static IP Address Settings, page 9-9](#)
- [Verifying Voice VLAN Configuration, page 9-10](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 9-10](#)
- [Eliminating DNS or Other Connectivity Errors, page 9-11](#)

Verifying Physical Connection

Verify that the Ethernet connection to which the Cisco IP Phone is connected is up. For example, check if the particular port or switch to which the phone is connected is down.

Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been 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 its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

Verifying DHCP Settings

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. See the [“Network Configuration Menu” section on page 4-6](#) for more information.
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 IP Phones 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 phone to restart and request a new IP address from the DHCP server.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the [“Network Configuration Menu” section on page 4-6](#) for more information.

Verifying Voice VLAN Configuration

If the Cisco 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.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the [“Understanding How the Cisco IP Phone Interacts with the Cisco Family of Switches”](#) section on page 2-3 for details.

Verifying that the Phones Have Not Been Intentionally Reset

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

You can check whether a Cisco IP Phone 7970 Series received a command from Cisco CallManager to reset by pressing the **Settings** button on the phone and choosing **Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- **Reset-Reset**—Phone closed due to receiving a Reset/Reset from Cisco CallManager administration.
- **Reset-Restart**—Phone closed due to receiving a Reset/Restart from Cisco CallManager administration.

Eliminating DNS or Other Connectivity Errors

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

-
- Step 1** Use the **Erase** softkey to reset phone settings to their default values. See the “[Resetting or Restoring the Cisco IP Phone](#)” section on page 9-15 for details.
- Step 2** Modify DHCP and IP settings.
- Disable DHCP. See the “[Network Configuration Menu](#)” section on page 4-6 for instructions.
 - Assign static IP values to the phone. See the “[Network Configuration Menu](#)” section on page 4-6 for instructions. Use the same default router setting used for other functioning Cisco IP Phones.
 - Assign TFTP server. See the “[Network Configuration Menu](#)” section on page 4-6 for instructions. Use the same TFTP server used for other functioning Cisco IP Phones.
- Step 3** On the Cisco CallManager server, verify that the local host files have the correct Cisco CallManager server name mapped to the correct IP address. Refer to *Configuring The IP Hosts File on a Windows 2000 CallManager Server*, available at this URL:
http://www.cisco.com/warp/customer/788/AVVID/cm_hosts_file.html
- Step 4** From Cisco CallManager, choose **System > Server** and verify that the server is referred to by its IP address and not by its DNS name.
- Step 5** From Cisco CallManager, choose **Device > Phone** and verify that you have assigned the correct MAC address to this Cisco IP Phone.
- For information about determining a MAC address, see the “[Determining the MAC Address of a Cisco IP Phone](#)” section on page 1-17.
- Step 6** Power cycle the phone.
-

Troubleshooting Cisco IP Phone Security

[Table 9-1](#) provides troubleshooting information for the security features on the Cisco IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*.

Table 9-1 Cisco IP Phone Security Troubleshooting

Problem	Possible Cause
Device authentication error.	CTL file does not have a Cisco CallManager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the CTL file.	Bad TFTP record.
Phone reports TFTP authorization failure.	<ul style="list-style-type: none"> The TFTP address for the phone does not exist in the CTL file. If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.
Phone does not register with Cisco CallManager.	The CTL file does not contain the correct information for the Cisco CallManager server.
Phone does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.

General Troubleshooting Tips

[Table 9-2](#) provides general troubleshooting information for the Cisco IP Phone.

Table 9-2 Cisco IP Phone Troubleshooting


Summary	Explanation
Daisy-chaining IP phones.	Do not connect an IP phone to another IP phone through the access port. Each IP phone should directly connect to a switch port. If you connect IP phones together in a line (daisy-chaining), a problem with one phone can affect all subsequent phones in the line. Also, all phones on the line share bandwidth.
Poor quality when calling digital cell phones using the G.729 protocol.	In Cisco CallManager, 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 digital cellular phone will have poor voice quality. Use G.729 only when absolutely necessary.
Prolonged broadcast storms cause IP phones to re-register.	Prolonged broadcast storms (lasting several minutes) on the voice VLAN cause the IP phones to re-register with another Cisco CallManager server.
Moving a network connection from the phone to a workstation.	<p>If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone's network connection and plug the cable into a desktop computer.</p>
	<p> Caution The computer's 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 there is no longer a phone on the line and to stop providing power to the cable.</p>
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 the “Unlocking and Locking Options” section on page 4-3 for details.

Table 9-2 Cisco IP Phone Troubleshooting (continued)

Summary	Explanation
Phone resetting.	The phone resets when it loses contact with the Cisco CallManager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.
LCD display issues.	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay.	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.
Codec mismatch between the phone and another device.	<p>The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco IP phone and the other device. These 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.</p> <p>See the “Call Statistics Screen” section on page 7-14 for information about displaying these statistics.</p>
Sound sample mismatch between the phone and another device.	<p>The RxSize and the TxSize statistics show the size of the voice packets that is being used a conversation between this Cisco IP phone and the other device. The values of these statistics should match.</p> <p>See the “Call Statistics Screen” section on page 7-14 for information about displaying these statistics.</p>
Gaps in voice calls.	<p>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.</p> <p>See the “Call Statistics Screen” section on page 7-14 for information about displaying these statistics.</p>

Resetting or Restoring the Cisco IP Phone

There are two methods for resetting or restoring the Cisco IP Phone:

- [Performing a Basic Reset, page 9-15](#)
- [Performing a Factory Reset, page 9-16](#)

Performing a Basic Reset

Performing a basic reset of a Cisco 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.

[Table 9-3](#) 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 9-3 Basic Reset Methods

Operation	Performing	Explanation
Restart phone	From any screen that does not accept user input, press **#** .	Resets to previously-saved settings any user and network configuration changes that you have made but that the phone has not written to its Flash memory, then restarts the phone.

Table 9-3 Basic Reset Methods (continued)

Operation	Performing	Explanation
Erase softkey	From the Settings menu, unlock phone options (see the “Unlocking and Locking Options” section on page 4-3). Then press the Erase softkey.	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 the “Unlocking and Locking Options” section on page 4-3). Then press the Erase softkey.	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 the “Unlocking and Locking Options” section on page 4-3). Then press the Erase softkey.	Deletes the CTL file from the phone and restarts the phone.

Performing a Factory Reset

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

- CTL file—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 term70.default.loads file)

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 its 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 yellow.
- 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 will not take place.
After you press these keys, the line buttons on the phone flash red and the phone goes through the factory reset process.
Do not power down the phone until it completes the factory reset process and the main screen appears.
-

Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco IP Phone 7970 Series. The QRT feature is installed as part of the Cisco CallManager installation.

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

When a user presses the **QRT** softkey, 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 whether the destination device is a Cisco IP Phone.

For more information about using QRT, refer to *Cisco CallManager Serviceability Administration Guide* and *Cisco CallManager Serviceability System Guide*.

Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco IP Phones, several Cisco.com web sites can provide you with more tips.

- Cisco IP Phone Troubleshooting Resources:
http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:IP_Phones&s=Troubleshooting
- Cisco Products and Technologies (Cisco Voice Applications, including Cisco CallManager):
http://www.cisco.com/warp/public/44/jump/voice_applications.shtml
- Cisco Products and Technologies (telephony, including Cisco IP Phones):
<http://www.cisco.com/warp/public/44/jump/telephony.shtml>

Cleaning the Cisco IP Phone

To clean your Cisco IP phone, use a soft, dry cloth to wipe the phone and the touchscreen. 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 touchscreen before cleaning it so that you will not inadvertently choose a feature from the pressure of the cleaning cloth. To disable the touchscreen so that it will not respond to touch, press the **Display** button for more than one second. The phone displays Touchscreen Disabled and the **Display** button flashes green.

After one minute, the touchscreen automatically re-enables itself. To re-enable the touchscreen before that, press the flashing **Display** button for more than one second. The phone displays Touchscreen Enabled.