Technical Details

- Physical and Operating Environment Specifications, page 1
- Cable Specifications, page 2
- Phone Power Requirements, page 4
- Network Protocols, page 7
- VLAN Interaction, page 11
- Cisco Unified Communications Manager Interaction, page 12
- Cisco Unified Communications Manager Express Interaction, page 12
- Voice Messaging System Interaction, page 13
- Phone Startup Overview, page 13
- External Devices, page 15
- USB Port Information, page 16
- Phone Configuration Files, page 16
- Network Bandwidth, page 17
- Phone Behavior During Times of Network Congestion, page 17

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

Table 1: Physical and Operating Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value or range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>32° to 104°F (0° to 40°C)</td>
</tr>
<tr>
<td>Operating relative humidity</td>
<td>10% to 95% (noncondensing)</td>
</tr>
</tbody>
</table>
### Technical Details

#### Cable Specifications

The following information lists the cable specifications:

- RJ-9 jack (4-conductor) for handset and headset connection
- RJ-45 jack for the LAN 10/100/1000BaseT connection (10/100/1000 Network port on the Cisco Unified IP Phone 8961, 9951, and 9971)
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (10/100/1000 Computer port on the Cisco Unified IP Phone 8961, 9951, and 9971)

---

---

---

---

---
- 3.5 mm jack for microphone and speaker connection (for Cisco Unified IP Phone 9951 and 9971 only)
- 48-volt power connector

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is the 10/100/1000 SW port on the Cisco Unified IP Phone.
- The computer (access) port is the 10/100/1000 PC port on the Cisco Unified IP Phone.

Network Port Connector

The following table describes the network port connector pinouts.

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>2</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DB+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DC-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DD-</td>
</tr>
</tbody>
</table>

**Note** BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.

Computer Port Connector

The following table describes the computer port connector pinouts.

---

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 10.0
### Table 3: Computer (Access) Port Connector Pinouts

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DB+</td>
</tr>
<tr>
<td>2</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DD-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DC-</td>
</tr>
</tbody>
</table>

**Note** BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.

### Phone Power Requirements

The Cisco Unified IP Phone 8961, 9951, and 9971 can be powered with external power or with Power over Ethernet (PoE). A separate power supply provides external power. The switch can provide PoE through the phone Ethernet cable.

**Note** When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

When connecting the phone to a Cisco switch which supports NG-PoE+, and both CDP and LLDP are enabled on the switch, disable the LLDP protocol on the phone from the Cisco Unified Communications Manager Administration.

The following table provides guidelines for Cisco Unified IP Phone 8961, 9951, and 9971 power.

### Table 4: Guidelines for Cisco Unified IP Phone 8961, 9951, and 9971 Power

<table>
<thead>
<tr>
<th>Power Type</th>
<th>Guidelines</th>
</tr>
</thead>
</table>
| External power: Provided through the CP-PWR-CUBE-4= external power supply | The Cisco Unified IP Phone 8961, 9951, and 9971 uses the CP-PWR-CUBE-4 power supply.  
**Note** You must use the CP-PWR-CUBE-4 when you deploy the Cisco Unified IP Phone 9971 on a wireless network. |
### Technical Details

**Phone Power Requirements**

<table>
<thead>
<tr>
<th>Power Type</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External power—Provided through the Cisco Unified IP Phone Power Injector.</td>
<td>The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.</td>
</tr>
</tbody>
</table>
| PoE power—Provided by a switch through the Ethernet cable attached to the phone. | Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs.  
Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3at for external add-on devices.  
To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.  
Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information.  
Support for NG-PoE+: The Cisco Unified IP Phone 8961, 9951, and 9971 can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support. |

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco Unified IP Phones
- Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions about power

<table>
<thead>
<tr>
<th>Document Topics</th>
<th>URL</th>
</tr>
</thead>
</table>
Power Outage

Your access to emergency service through the phone requires that the phone receive power. If a power interruption occurs, service or emergency calling service dialing does not function until power is restored. If a power failure or disruption occurs, you may need to reset or reconfigure the equipment before you can use service or emergency calling service dialing.

Power Reduction

You can reduce the amount of energy that the Cisco IP Phone consumes by using Power Save or EnergyWise (Power Save Plus) mode.

Power Save

In Power Save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in Power Save mode for the scheduled duration or until the user lifts the handset or presses any button.

Set up each phone to enable or disable Power Save settings. You can configure the phones to dim the backlight on a schedule.

Power Save Plus (EnergyWise)

The Cisco IP Phone supports Cisco EnergyWise (Power Save Plus) mode. When your network contains an EnergyWise (EW) controller (for example, a Cisco switch with the EnergyWise feature enabled), you can configure these phones to sleep (power down) and wake (power up) on a schedule to further reduce power consumption.

Set up each phone to enable or disable the EnergyWise settings. If EnergyWise is enabled, configure a sleep and wake time, as well as other parameters. These parameters are sent to the phone as part of the phone configuration XML file.

Power Negotiation over LLDP

The phone and the switch negotiate the power that the phone consumes. Cisco Unified IP Phone 8961, 9951, and 9971 operates at multiple power settings, which lowers power consumption when less power is available.

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. The switch locks to the first protocol (containing a power Threshold Limit Value [TLV]) that the phone transmits. If the system administrator disables that protocol on the phone, the phone cannot power up any accessories because the switch does not respond to power requests in the other protocol.

Cisco recommends that Power Negotiation always be enabled (default) when connecting to a switch that supports power negotiation.

If Power Negotiation is disabled, the switch may disconnect power to the phone. If the switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power the accessories up to the maximum that the IEEE 802.3af-2003 standard allows.
Network Protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified IP Phone 8961, 9951, and 9971 support.

Table 5: Supported network protocols on the Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Network protocol</th>
<th>Purpose</th>
<th>Usage notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.</td>
<td>Cisco Unified IP Phones 9951 and 9971 support Bluetooth 2.1.</td>
</tr>
<tr>
<td>Bootstrap Protocol (BootP)</td>
<td>BootP enables a network device, such as the Cisco Unified IP Phone, to discover certain startup information, such as the IP address.</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Audio Session Tunnel (CAST)</td>
<td>The CAST protocol allows Cisco Unified IP Phones and associated applications to discover and communicate with the remote IP Phones without requiring changes to the traditional signaling components, such as Cisco Unified Communications Manager (CM) and gateways.</td>
<td>The Cisco Unified IP Phone uses CAST as an interface between CUVA and Cisco Unified Communications Manager using the Cisco Unified IP Phone as a SIP proxy.</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</td>
<td>The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.</td>
</tr>
<tr>
<td>Cisco Peer-to-Peer Distribution Protocol (CPPDP)</td>
<td>CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.</td>
<td>CPPDP is used by the Peer Firmware Sharing feature.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and the phone to become operational without the need to manually assign an IP address or to configure additional network parameters.</td>
<td>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the “Dynamic Host Configuration Protocol” chapter and the “Cisco TFTP” chapter in the Cisco Unified Communications Manager System Guide. <strong>Note</strong> If you cannot use option 150, you may try using DHCP option 66.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol (HTTP)</td>
<td>HTTP is the standard way of transferring information and moving documents across the Internet and the web.</td>
<td>Cisco Unified IP Phones use HTTP for XML services and for troubleshooting purposes.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol Secure (HTTPS)</td>
<td>Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.</td>
<td>Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
<td>The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.</td>
<td>The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN.</td>
</tr>
<tr>
<td>IEEE 802.11a/b/g</td>
<td>The IEEE 802.11 standard specifies how devices communicate over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band and 802.11b and 802.11g operate at the 2.4 GHz band</td>
<td>(Cisco Unified IP Phone 9971 only) The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet Protocol (IP)</td>
<td>IP is a messaging protocol that addresses and sends packets across the network.</td>
<td>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phones support IPv6 addresses. For more information, see <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Internet Protocol Version 6 (IPv6)&quot; chapter.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.</td>
<td>The Cisco Unified IP Phone supports LLDP on the PC port.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)</td>
<td>LLDP-MED is an extension of the LLDP standard for voice products.</td>
<td>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the LLDP-MED and Cisco Discovery Protocol white paper: <a href="http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml">http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml</a></td>
</tr>
<tr>
<td>Real-Time Transport Protocol (RTP)</td>
<td>RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.</td>
<td>Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Real-Time Control Protocol</strong></td>
<td><strong>RTCP</strong> works in conjunction with <strong>RTP</strong> to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams.</td>
<td><strong>RTCP</strong> for audio calls is disabled by default. <strong>RTCP</strong> for video calls (including both audio streams and video streams in the video call) is enabled by default. You can enable or disable <strong>RTCP</strong> on individual phones from the Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td><strong>Session Description Protocol</strong></td>
<td><strong>SDP</strong> is the portion of the <strong>SIP</strong> protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the <strong>SDP</strong> capabilities that all endpoints in the conference support.</td>
<td><strong>SDP</strong> capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some <strong>SIP</strong> endpoints may allow configuration of these parameters on the endpoint itself.</td>
</tr>
<tr>
<td><strong>Session Initiation Protocol</strong></td>
<td><strong>SIP</strong> is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. <strong>SIP</strong> is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.</td>
<td><strong>SIP</strong> is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. <strong>SIP</strong> addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. Cisco Unified IP Phones support the <strong>SIP</strong> protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.</td>
</tr>
<tr>
<td><strong>Transmission Control Protocol</strong></td>
<td><strong>TCP</strong> is a connection-oriented transport protocol.</td>
<td>Cisco Unified IP Phones use <strong>TCP</strong> to connect to Cisco Unified Communications Manager and to access XML services.</td>
</tr>
<tr>
<td><strong>Transport Layer Security</strong></td>
<td><strong>TLS</strong> is a standard protocol for securing and authenticating communications.</td>
<td>Upon security implementation, Cisco Unified IP Phones use the <strong>TLS</strong> protocol when securely registering with Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
### VLAN Interaction

The Cisco Unified IP Phone 8961, 9951, and 9971 contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured for separate VLANs for carrying:

---

### Technical Details

#### VLAN Interaction

The Cisco Unified IP Phone 8961, 9951, and 9971 contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured for separate VLANs for carrying:

---

### Related Topics

- 802.1X Authentication
- Configure Network Settings
- Phone Startup Process
- VLAN Interaction, on page 11
- Cisco Unified Communications Manager Interaction, on page 12
- Cisco Unified Communications Manager Express Interaction, on page 12
- Set Up the Audio and Video Port Range
• Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
• Data traffic to and from the PC that connects to the switch through the computer (access) port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network that does not have enough IP addresses for each phone.

For more information, see the documentation that is included with a Cisco switch. You can also access switch information at this URL:

Related Topics
Network Protocols, on page 7

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

• Firmware for phones
• Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP service
• Phone registration
• Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note
If the Cisco IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, install the latest support patch for your version of Cisco Unified Communications Manager from Cisco.com.

Related Topics
Network Protocols, on page 7

Cisco Unified Communications Manager Express Interaction

When the Cisco IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones must go into CME mode.
When a user invokes the conference feature, the tag allows the phone to use either a local or network hardware conference bridge.

The Cisco IP Phones do not support the following actions:

- Transfer: Only supported in the connected call transfer scenario.
- Conference: Only supported in the connected call transfer scenario.
- Join: Supported using the Conference button or hookflash access.
- Hold: Supported using the Hold button.
- Barge: Not supported.
- Direct Transfer: Not supported.
- Select: Not supported.

The users cannot create conference and transfer calls across different lines.

**Related Topics**

Network Protocols, on page 7

---

**Voice Messaging System Interaction**

Cisco Unified Communications Manager lets you integrate with different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide the following information to each user:

- How to access the voice messaging system account.
  
  Make sure that you have used Cisco Unified Communications Manager to configure the Messages button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.
  
  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.
  
  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

---

**Phone Startup Overview**

When connecting to the VoIP network, the Cisco Unified IP Phone 8961, 9951, and 9971 goes through a standard startup process. Depending on your specific network configuration, only some of these steps may occur on your Cisco Unified IP Phone.

1. Obtain power from the switch. If a phone is not using external power, the switch provides inline power through the Ethernet cable that is attached to the phone.
2 (For a Cisco Unified IP Phone 9971 in a wireless LAN only) Scan for an access point. The Cisco Unified IP Phone 9971 scans the RF coverage area with the radio. The phone searches the network profiles and scans for access points that contain a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with the network profile.

3 (For a Cisco Unified IP Phone 9971 in a wireless LAN only) Authenticate with the access point. The Cisco Unified IP Phone begins the authentication process. The following table describes the authentication process:

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Key Management Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>None</td>
<td>Any device can authenticate to the access point. For added security, static WEP encryption might optionally be used.</td>
</tr>
<tr>
<td>Shared Key</td>
<td>None</td>
<td>The phone encrypts the challenge text by using the WEP key and the access point must verify the WEP key that was used to encrypt the challenge text before network access is available.</td>
</tr>
<tr>
<td>LEAP or EAP-FAST</td>
<td>None</td>
<td>The RADIUS server authenticates the username and password before network access is available.</td>
</tr>
<tr>
<td>Auto (AKM)</td>
<td>WPA, WPA2, or CCKM</td>
<td>The phone looks for an access point with one of the key management options enabled. The username and password are authenticated by the RADIUS server before network access is available.</td>
</tr>
<tr>
<td>Auto (AKM)</td>
<td>WPA-Pre-shared key, WPA2-Pre-shared key</td>
<td>The phone looks for an access point that has one of the key management options enabled. Authentication uses the configured WPA-Pre-shared key or WPA2-Pre-shared key</td>
</tr>
</tbody>
</table>

4 Load the stored phone image. The Cisco Unified IP Phone has nonvolatile flash memory in which the phone stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone firmware image that is stored in flash memory. Using this image, the phone initializes the software and hardware.

5 Configure the VLAN. If the Cisco Unified IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN that is defined on the switch. The phone needs to know the VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.

6 Obtain an IP address. If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.

7 Request the CTL file. The TFTP server stores the CTL file. This file contains the certificates that are necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.
For more information, see the Cisco Unified Communications Manager Security Guide, "Configuring the Cisco CTL Client" chapter.

8 Request the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

9 Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly.

Note
You can also assign an alternate TFTP server to use instead of the one that DHCP assigns.

10 Request the configuration file. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.

11 Contact Cisco Unified Communications Manager. The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified CM and provides a phone with the load ID. After it obtains the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified CM on the list.

If the security profile of the phone is configured for secure signaling (encrypted or authenticated) and the Cisco Unified Communications Manager is set to secure mode, the phone makes a TLS connection. Otherwise, the phone makes a nonsecure TCP connection.

If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and autoregistration is enabled in Cisco Unified Communications Manager, the phone attempts to autoregister itself in the Cisco Unified Communications Manager database.

Note
Autoregistration is disabled when you configure the CTL client. In this case, you must add the phone to the Cisco Unified Communications Manager database manually.

External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, we recommend that you take one or more of these actions:

• Move the external device away from the source of the RF or AF signals.
• Route the external device cables away from the source of the RF or AF signals.
• Use shielded cables for the external device, or use cables with a better shield and connector.
• Shorten the length of the external device cable.
• Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of external devices, cables, and connectors.

**Caution**

In European Union countries, use only external speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].

---

**USB Port Information**

The Cisco Unified IP Phone supports a maximum of five devices that connect to each USB port. Each device that connects to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port. The Cisco Unified IP Phone 8961 does not contain a back USB port. Many third-party USB products count as multiple USB devices; for example, a device containing a USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

**Note**

• Unpowered hubs are not supported, and powered hubs with more than four ports are not supported.

• USB headsets that connect to the phone through a USB hub are not supported.

• The Cisco Unified Video Camera that connects to the phone through a USB hub is not supported.

---

**Phone Configuration Files**

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone configuration file. Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the documentation for your particular Cisco Unified Communications Manager release. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when the following conditions exist:

• You have enabled autoregistration in Cisco Unified Communications Manager

• The phone has not been added to the Cisco Unified Communications Manager database

• The phone is registering for the first time
Network Bandwidth

When using secure video over VPN and VXC/VPN, the maximum supported bandwidth is 320 kpbs. When the phone calls Cisco TelePresence, the maximum bandwidth is 320 kbps.

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP 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
Phone Behavior During Times of Network Congestion