# Technical Details


- Physical and Operating Environment Specifications, page 1
- Cable Specifications, page 2
- Phone Power Requirements, page 2
- Supported Network Protocols, page 3
- External Devices, page 6
- Phone Behavior During Times of Network Congestion, page 7


## Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the conference phone.

***Table 1: Physical and Operating Specifications***

| Specification | Value or Range |
|---|---|
| Operating temperature | 32° to 104°F (0° to 40°C) |
| Operating relative humidity | 10% to 90% (noncondensing) |
| Storage temperature | 14° to 140°F (–10° to 60°C) |
| Height | 8.9 in. (226 mm) |
| Width | 8.9 in. (226 mm) |
| Depth | 2.14 in. (54.4 mm) |
| Weight | 2.0 lb. (0.907 kg) |

| Specification | Value or Range |
|---|---|
| Power | • IEEE PoE Class 2. The phone is compatible with both IEEE 802.3af and 802.3at switch blades and supports both Cisco Discovery Protocol and Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE)<br>• If the connected LAN switches don't support PoE, an additional PoE power injector will be needed to convert AC wall power to provide PoE |
| Cables | Category 3/5/5e/6 for 10-Mpbs cables with 4 pairs<br>Category 5/5e/6 for 100-Mbps cables with 4 pairs<br>**Note** Cables have 4 pairs of wires for a total of 8 conductors. |
| Distance Requirements | The Ethernet Specification assumes that the maximum cable length between each conference phone and the switch is 100 meters (330 feet). |

For more information, see the *Cisco IP Conference Phone 7832 Data Sheet*: http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/datasheet-listing.html

# Cable Specifications

- RJ-45 jack for the LAN 10/100BaseT connection.

# Phone Power Requirements

The Cisco IP Conference Phone can use these power sources:

- Power over Ethernet (PoE)
- Cisco IP Conference Phone 7832 PoE Midspan Cable and Cisco Power Cube 3
- Cisco IP Phone Power Injector

**Note** The midspan cable is not currently available.

*Table 2: Guidelines for Cisco IP Conference Phone Power*

| Power Type | Guidelines |
|---|---|
| PoE power—Provided by a switch through the Ethernet cable attached to the phone. | To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.<br>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. |
| External power—Provided through the Cisco IP Conference Phone 7832 PoE Midspan Cable and Cisco Power Cube 3 | The midspan cable and power cube provide power to the Ethernet cable.<br>When you install a phone that is powered with the midspan adapter, connect the adapter to power before you connect the Ethernet cable to the phone. When you remove a phone that uses the midspan adapter, disconnect the Ethernet cable from the phone before you remove the power from the adapter. |
| External power—Provided through the Cisco IP Phone Power Injector | The power injector provides power to the Ethernet cable.<br>When you install a phone that is powered with the power injector, connect the injector to power before you connect the Ethernet cable to the phone. When you remove a phone that uses the injector, disconnect the Ethernet cable from the phone before you remove the power from the injector. |

## 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.

# Supported Network Protocols

Cisco IP Conference Phones support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the phones support.

*Table 3: Supported Network Protocols on the Cisco IP Conference Phone*

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Bootstrap Protocol (BootP) | BootP enables a network device, such as the phone, to discover certain startup information, such as its IP address. | — |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Cisco Discovery Protocol (CDP) | CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.<br>A device can use CDP to advertise its existence to other devices and receive information about other devices in the network. | The 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. |
| Dynamic Host Configuration Protocol (DHCP) | DHCP dynamically allocates and assigns an IP address to network devices.<br>DHCP enables you to connect an IP phone into the network and have the phone become operational without the need to manually assign an IP address or to configure additional network parameters. | 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.<br>We recommend 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 documentation for your particular Cisco Unified Communications Manager release.<br>**Note** If you cannot use option 150, use DHCP option 66. |
| Hypertext Transfer Protocol (HTTP) | HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web. | Phones use HTTP for XML services, provisioning, upgrade and for troubleshooting purposes. |
| Hypertext Transfer Protocol Secure (HTTPS) | 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. | Web applications with both HTTP and HTTPS support have two URLs configured. phones that support HTTPS choose the HTTPS URL.<br>A lock icon is displayed to the user if the connection to the service is via HTTPS. |
| IEEE 802.1X | The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connection to a LAN through publicly accessible ports.<br>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. | The phone implements the IEEE 802.1X standard through support for the following authentication methods: EAP-FAST and EAP-TLS.<br>When 802.1X authentication is enabled on the phone, you should disable the voice VLAN. |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Internet Protocol (IP) | IP is a messaging protocol that addresses and sends packets across the network. | To communicate with IP, network devices must have an assigned IP address, subnet, and gateway.<br>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.<br>The phones support IPv6 address. For more information, see the documentation for your particular Cisco Unified Communications Manager release. |
| Link Layer Discovery Protocol (LLDP) | LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices. | |
| Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) | LLDP-MED is an extension of the LLDP standard developed for voice products. | The phone supports LLDP-MED on the SW port to communicate information such as:<br>• Voice VLAN configuration<br>• Device discovery<br>• Power management<br>• Inventory management<br>For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper at this URL: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml |
| Real-Time Transport Protocol (RTP) | RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks. | Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways. |
| Real-Time Control Protocol (RTCP) | RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams. | RTCP is enabled by default. |

| Network Protocol | Purpose | Usage Notes |
|---|---|---|
| Session Initiation Protocol (SIP) | SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP 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. | Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. |
| Secure Real-Time Transfer protocol (SRTP) | SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints. | Phones use SRTP for media encryption. |
| Transmission Control Protocol (TCP) | TCP is a connection-oriented transport protocol. | Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services. |
| Transport Layer Security (TLS) | TLS is a standard protocol for securing and authenticating communications. | When security is implemented, phones use the TLS protocol when securely registering with the Cisco Unified Communications Manager. For more information, see the documentation for your particular Cisco Unified Communications Manager release. |
| Trivial File Transfer Protocol (TFTP) | TFTP allows you to transfer files over the network.<br>On the phone, TFTP enables you to obtain a configuration file specific to the phone type. | TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Setup menu on the phone.<br>For more information, see the documentation for your particular Cisco Unified Communications Manager release. |
| User Datagram Protocol (UDP) | UDP is a connectionless messaging protocol for delivery of data packets. | Phones transmit and receive RTP streams, which utilize UDP. |

# 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].

# 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