Technical Details

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	10.9 inches (278 mm)
Width	10.9 inches (278 mm)
Depth	2.4 inches (61.3 mm)
Weight	4.07 lb. (1852 g)
Power	IEEE PoE Class 3 via a PoE injector. The phone is compatible with Protocol and Link Layer Discovery Protocol - Power over Etherne Other options include a non-PoE Ethernet injector if the connected Phone 8832 Power Adapter is needed.

Specification	Value or Range
Security features	Secure boot
Cables	USB-C
Distance Requirements	The Ethernet Specification assumes that the maximum cable length be

For more information, see the *Cisco IP Conference Phone 8832 Data Sheet*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Phone Power Requirements

The Cisco IP Conference Phone 8832 can use these power sources:

- Power over Ethernet (PoE) deployment with a Cisco IP Conference Phone 8832 PoE Injector
- Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector
- Wi-Fi deployment with a Cisco IP Conference Phone 8832 Power Adapter

Table 2: Guidelines for Cisco IP Conference Phone Power

Power Type	Guidelines
PoE power—Provided by either the Cisco IP Conference Phone 8832 PoE Injector or Cisco IP Conference Phone 8832 Ethernet Injector through the USB-C cable attached to the phone.	If you are using either the Cisco IP Conference Phone 8832 PoE Injector or Cisco IP Conference Phone 8832 Ethernet Injector, make sure that the switch has a backup power supply to ensure uninterruptible operation of the phone. Ensure 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. When you install a phone that is powered by PoE, connect the injector to the LAN before you connect the USB-C cable to the phone. When you remove a phone that uses PoE, disconnect the USB-C cable from the phone before you remove the power from the adapter.

Power Type	Guidelines
External power • Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector • Wi-Fi deployment with a Cisco IP Conference Phone 8832 Power Adapter • Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Ethernet Injector and a Cisco IP Conference Phone 8832 Power Adapter	When you install a phone that is powered with external power, connect the injector to power and to the Ethernet before you connect the USB-C cable to the phone. When you remove a phone that uses external power, disconnect the USB-C cable from the phone before you remove the power from the adapter.

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 presses any button.

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.

Related Topics

Schedule Power Save for Cisco IP Phone
Schedule EnergyWise on Cisco IP Phone

Network Protocols

The Cisco IP Conference Phone 8832 supports 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.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. 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 s of Service (QoS) configuration information with the
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. 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 r on each phone locally. We recommend that you use DHCP custom option 1 value. For additional supported DHCP configuration Manager release. **Note** If you cannot use option 150, use DHC
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,
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 suppo URL. A lock icon is displayed to the user if the connection
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. 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 th EAP-TLS. When 802.1X authentication is enabled on the phon
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate with IP, network devices must hav IP addresses, subnets, and gateways identifications Configuration Protocol (DHCP). If you are not usin The phones support IPv6 address. For more informa Manager release.

Network Protocol	Purpose	Usage Notes
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.	The phone supports LLDP on the PC port.
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 por • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED suppor https://www.cisco.com/en/US/tech/tk652/tk701/
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 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.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF de Unified Communications Manager or Media Gate on the endpoint itself.
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 add network. Signaling allows call information to be 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 Co
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, phones use the T Manager. For more information, see the docume
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, v to use a TFTP server other than the one specified by using the Network Setup menu on the phone. For more information, see the documentation fo

Network Protocol	Purpose	Usage Notes
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling or

Related Topics

Cisco Unified Communications Manager Documentation

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 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 and HTTP services
- 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 phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the 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 device package for your version of Cisco Unified Communications Manager from Cisco.com.

Related Topics

Cisco Unified Communications Manager Documentation

Cisco Unified Communications Manager Express Interaction

When your phone works with the Cisco Unified Communications Manager Express (Unified CME), it 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 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 and Merge—Not supported.
- Direct Transfer—Not supported.
- Select—Not supported.

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

Unified CME supports intercom calls, also known as whisper paging. But the page is rejected by the phone during calls.

Voice Messaging System Interaction

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

To enable the ability for a user to transfer to voicemail, set up a *xxxxx dialing pattern and configure it as Call Forward All to Voicemail. For more information, see the Cisco Unified Communications Manager documentation.

Provide the following information to each user:

- How to access the voice messaging system account.

  Make sure that you have used the Cisco Unified Communications Manager to configure the Messages button on the Cisco IP Phone.

- Initial password for accessing the voice messaging system.

  Configure a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

  Use Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

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

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio 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.

Application Programming Interface

Cisco supports phone API utilization by 3rd party applications that have been tested and certified through Cisco by the 3rd party application developer. Any phone issues related to uncertified application interaction must be addressed by the 3rd party and will not be addressed by Cisco.

For support model of Cisco certified 3rd party applications/solutions, please refer to Cisco Solution Partner Program website for details.