Technical Details

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified SIP Phone 3905.

Table 1: Physical and Operating Environment Specifications for the Cisco Unified SIP Phone 3905

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (noncondensing)
Storage temperature	14° to 140°F (-10° to 60°C)
Height	8.07 in. (20.5 cm)
Width	5.91 in. (15.0 cm)
Depth	2.11 in. (5.35 cm) - Excluding the handset

Specification	Value or Range
Weight	• 0.987 lb (447.8 g) - Phone without handset • 0.347 lb (157.6 g) - Handset weight
Power	• 100-240 VAC, 50-60 Hz, 0.5 A - When using the AC adapter • 48 VDC, 0.2 A - When using the in-line power over the network cable
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified SIP Phone 3905).
- RJ-45 jack for a second 10/100BaseT compliant connection.
- 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 labeled `Network` on the phone.
- The computer (access) port is labeled `Computer` on the phone.

Network Port Connector

The following table describes the network port connector pinouts.

Table 2: Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
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.

Table 3: Computer (Access) Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
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 SIP Phone 3905 can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

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.

The following table provides guidelines for powering the Cisco Unified SIP Phone 3905.

Table 4: Cisco Unified SIP Phone 3905 power guidelines

Power Type	Guidelines
External power: Provided through the Cisco Unified SIP Phone 3905 Power Adapter.	The Cisco Unified SIP Phone 3905 uses the Cisco Unified SIP Phone 3905 Power Adapter.
External power: Provided through the Cisco Unified IP Phone Power Injector.	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 is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.
PoE power: Provided by a switch through the Ethernet cable attached to the phone.	• The Cisco Unified SIP Phone 3905 supports IEEE 802.3af Class 1 power on signal pairs and spare pairs. • 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 running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.
External power: Provided through inline power patch panel WS-PWR-PANEL	The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified SIP Phone 3905.

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.

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.

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 SIP Phone 3905 support.

Table 5: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	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.	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. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing 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. 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, go to the "Dynamic Host Configuration Protocol" chapter and the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	The DHCPv6 server assigns an IPv6 address to the phone.	You must disable DHCPv6 to edit IPv6 Setup menu options.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for troubleshooting purposes.
IEEE 802.1X	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.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the MD5 authentication method. When 802.1X authentication is enabled on the phone, you should disable the voice VLAN.

Network Protocol	Purpose	Usage Notes
Internet Control Message Protocol for IPv6 (ICMPv6)		
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways 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 Phone supports IPv6 addresses. For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Internet Protocol Version 6 (IPv6)" chapter.
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 Cisco Unified IP Phone supports LLDP on the switch and 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 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: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.

Network Protocol	Purpose	Usage Notes
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 disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager.
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. Cisco Unified IP Phones support the SIP protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP 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 Configuration menu on the phone. For more information, go to the “Cisco TFTP” chapter in the *Cisco Unified Communications Manager System Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

Cisco Unified Communications Manager Interaction, on page 5

VLAN Interaction

The Cisco Unified SIP Phone 3905 has an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

If a computer is connected to the 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 connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of Voice-over-IP 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 that the phone is connected to would be configured to have separate VLANs for carrying:

- 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 connected to the switch through the 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 where there are not enough IP addresses for each phone.

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

http://cisco.com/en/US/products/hw/switches/index.html

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