Technical Specifications

Physical and Operating Environment Specifications

Table 1: Physical and Operating Specifications for Cisco DX Series Devices

Specification	Value or Range
Physical dimensions (H x W x D)	Cisco DX70: 14.84 in. (377.1 mm) x 13.91 in. (353.1 mm) x 2.45 in. (62.3 mm) Cisco DX80: 20.2 in. (51 2mm) x 22.2 in. (565 mm) x 3.5 in. (89 mm) Cisco DX650: 8.46 in. (215 mm) x 10.35 in. (263 mm) x 8.19 in. (208 mm)
Weight	Cisco DX70: 8.5 lb (3.9 kg) Cisco DX80: 15.65 lb (7.1 kg) Cisco DX650: 3.81 lb (1.73 kg)
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)

Specification	Value or Range
Power, Cisco DX70	Rated: 3.5A at 12V maximum Low Power Standby mode Integrated EnergyWise support
Power, Cisco DX80	Rated: 60 W maximum Low Power Standby mode Integrated EnergyWise support
Power, Cisco DX650	IEEE 802.3af (Class 3) or IEEE 802.3at (Class 4) Power over Ethernet (PoE) standards are supported. Compatible with both Cisco Discovery Protocol and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) PoE switch blades. Power budget: 13.7W (Cisco Discovery Protocol) or 15.1W (LLDP) for 802.3AF and low-power USB peripheral support; greater than 15.4W and 802.3AT required for high-power USB peripheral support.
Connectivity	Internal 2-port Cisco Ethernet switch IEEE 802.11 a/b/g/n Wi-Fi
Audio codec support	Narrowband audio compression codecs: G.711a, G.711u, G.729a, G.729ab, and Internet Low Bitrate Codec (iLBC) Wideband audio compression codecs: G.722, Internet Speech Audio Codec (iSAC), iLBC, and AAC-LD audio compression codecs.
Operating System	Android™ 4.1.1 (Jellybean)
Processor	Cisco DX70: TI OMAP 4470 1.5GHz dual-core ARM Cortex-A9 processor Cisco DX80: TI OMAP 4470 1.5GHz dual-core ARM Cortex-A9 processor Cisco DX650: TI OMAP 4460 1.5-GHz dual-core ARM Cortex-A9 processor
Memory	2-GB RAM; Low Power Double Data Rate Synchronous Dynamic Random-Access Memory (LPDDR2 SDRAM)
Storage	8-GB eMMC NAND Flash memory (embedded multimedia card; nonvolatile)

Network and Computer Port Pinouts

Cisco DX Series devices include network and computer (access) ports, which are used for network connectivity. They serve different purposes and have different port pinouts.

- The network port is the 10/100/1000 SW port.
- The computer (access) port is the 10/100/1000 PC port.

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-
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 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-

Pin Number	Function
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.

Ports Used by Cisco DX Series Devices

The following table describes the ports that Cisco DX Series devices use. For additional information, see the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager*.

Table 4: Cisco DX Series Device Ports

Source Port	Remote Device Port	Underlying Protocol	Protocol/Service	Notes
68	67	-	DHCP client	DHCP support to obtain dynamic IP addresses
49152-53248	53	UDP	DNS client	DNS support for name resolution
49152-53248	69	UDP	TFTP client	TFTP support is required to obtain various configuration and image files from a central server.
49152-53248	80	TCP/UDP	HTTP client	
80	Server configured	TCP/UDP	HTTP server	
123	123	UDP	NTP client	Network Time Protocol to obtain time-of-day
49152-53248	Server configured	TCP	HTTP client	
49152-53248	6970	TCP	TFTP client	TFTP support is required to obtain various configuration and image files from a central server.
49152-53248	5060	TCP	SIP/TCP	Default is 5060; administrator can change.
49152-53248	5061	TCP	SIP/TLS	Default is 5061; administrator can change.

Source Port	Remote Device Port	Underlying Protocol	Protocol/Service	Notes
16384- 32767	Receiver Range	UDP	RTP	Administrator can configure port range.
16384- 32767	Receiver Range	UDP	RTCP	RTCP port is RTP +1.
4224	PC Dynamic Range	TCP		
22	Server configured	TCP	Secure shell	
4051		TCP		Load upgrades
4052		RDP		Load upgrades
4061				Special debugs
8443				Contacts search

Network Protocols

Cisco DX Series devices 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 devices support.

Table 5: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Binary Floor Control Protocol (BFCP)	BFCP allows users to share a presentation within an ongoing video conversation.	BFCP is automatically enabled.
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	The devices support Bluetooth 3.0. The devices support Hands-Free Profile (HFP), Advanced Audio Distribution (A2DP) Profile, Human Interface Device Profile (HID), Object Push Profile (OPP), and Phone Book Access Profile (PBAP).
Bootstrap Protocol (BootP)	BootP enables a network device to discover certain startup information, such as the IP address.	—

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 device 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.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol that is 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.	The Peer Firmware Sharing feature uses CPPDP.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect a device into the network and for that device to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If it is disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each device 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*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Devices use HTTP for XML services 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. Devices that support HTTPS choose the HTTPS URL.

Network Protocol	Purpose	Usage Notes
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 succeeds, normal traffic can pass through the port.	Devices implement the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST and EAP-TLS. When 802.1X authentication is enabled on the device, you should disable the PC port and voice VLAN.
IEEE 802.11a/b/g/n	The IEEE 802.11 standard specifies how devices communication 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. 802.11.n operates in either 2.4 GHz or 5Ghz band.	The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.
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, domain name, gateway, and netmask. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the device with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each device locally. The device supports IPv6 addresses. For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*, "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 device supports LLDP on the PC port.

Network Protocol	Purpose	Usage Notes
Link Layer Discovery Protocol - Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard for voice products.	The device 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/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.	The device uses 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 also used to synchronize the audio and video stream in order to provide a better video experience.	RTCP for audio calls is disabled by default. RTCP for video calls (including both audio streams and video streams in the video call) is enabled by default. You can enable or disable RTCP on individual devices from Cisco Unified Communications Manager Administration.
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 detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.

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 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.
Telepresence Interoperability Protocol (TIP)/Multiplex (MUX)	TIP/MUX is an IP protocol that is used to negotiate audio and video media options between endpoints prior to reception or transmission of media.	TIP/MUX is invoked for multiparticipant conferences and enables content sharing.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	The device uses 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.	Upon security implementation, the device uses the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the device, TFTP enables you to obtain a configuration file specific to the device type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify. If you want a device to use a TFTP server other than the one that the DHCP server specifies, you must manually assign the IP address of the TFTP server by using the Settings application on the device. For more information, see 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.	UDP is used only for RTP streams. SIP signaling on the devices does not support UDP.

Power Requirements

Cisco DX Series devices are powered with external power. A separate power supply provides external power.

Cisco DX650 can also be powered with Power over Ethernet (PoE). The switch can provide PoE through an Ethernet cable.

Note When you install a device 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 device. When you remove a device that is powered with external power, disconnect the Ethernet cable from the device before you disconnect the power supply.

Power Guidelines

To power the Cisco DX70 and the Cisco DX80, use the provided Lite-On PA-1600-2A-LF power supply or FSP075-DMAA1. To power the Cisco DX650, see the table below.

Table 6: Guidelines for Cisco DX650 Power

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-4= external power supply	The device uses the CP-PWR-CUBE-4 power supply. **Note** You must use the CP-PWR-CUBE-4 when you deploy the device on a wireless network.
External power—Provided through the Cisco Unified IP Phone Power Injector	The Cisco Unified IP Phone Power Injector may be used with any Cisco DX650. 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 phone, and supports a maximum cable length of 100m between the unpowered switch and the phone.
PoE power—Provided by a switch through the Ethernet cable that is attached to the phone	Cisco DX650 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs. These devices support 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 devices can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support.

Power Reduction

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

Power Save Mode

In Power Save mode, the backlight on the screen is not lit when the device is not in use. The device remains in Power Save mode for the scheduled duration or until the user lifts the handset or presses any button. In the Product Specific Configuration area of the **Phone Configuration** window on Cisco Unified Communications Manager, configure the following parameters:

Days Display Not Active

Specifies the days that the backlight remains inactive.

Display on Time

Schedules the time of day that the backlight automatically activates.

Display on Duration

Indicates the length of time that the backlight is active after the backlight is enabled by the programmed schedule.

EnergyWise Mode

In addition to Power Save mode, the device 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 devices to sleep (power down) and wake (power up) on a schedule to further reduce power consumption.

Set up each device 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 device as part of the configuration XML file. In the **Phone Configuration** window in Cisco Unified Communications Manager, configure the following parameters:

Enable Power Save Plus

Selects the schedule of days for which the device powers down.

Phone On Time

Determines when the device automatically turns on for the days that are selected in the **Enable Power Save Plus** field.

Phone Off Time

Determines the time of day that the device powers down for the days that are selected in the **Enable Power Save Plus** field.

Phone Off Idle Timeout

Determines the length of time that the device must be idle before it powers down.

Enable Audio Alert

When enabled, instructs the device to play an audible alert that starts 10 minutes before the time that the **Phone Off Time** field specifies.

EnergyWise Domain

Specifies the EnergyWise domain that the device is in.

EnergyWise Secret

Specifies the security secret password that is used to communicate within the EnergyWise domain.

Allow EnergyWise Overrides

Determines whether you allow the EnergyWise domain controller policy to send power-level updates to the devices.

When a device is sleeping, the power sourcing equipment (PSE) provides minimal power to the device to illuminate the **Power/Lock** button, and the **Power/Lock** button can be used to wake up the device when it is sleeping.

Power Negotiation Over LLDP

The device and the switch negotiate the power that the device consumes. Devices operate at multiple power settings, which lowers power consumption when less power is available.

After a device 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 device transmits. If the system administrator disables that protocol on the device, the device 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 the device connects to a switch that supports power negotiation.

If Power Negotiation is disabled, the switch may disconnect power to the device. 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 device can power the accessories up to the maximum that the IEEE 802.3af-2003 standard allows.

Note When CDP and Power Negotiation are disabled, the device can power the accessories up to 15.4 W.

Additional Information About Power

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

Document Topic	URL
Cisco Unified IP Phones Power Injector	http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-power-injector/index.html

Document Topic	URL
PoE Solutions	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
Cisco Catalyst Switches	http://www.cisco.com/cisco/web/psa/default.html?mode=prod http://www.cisco.com/c/en/us/products/switches/index.html
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/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.

Note Not all Cisco IP telephony products support external devices, cords, or cables. For more information, consult the documentation for your endpoint.

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 and USB Serial Console Data Information

Cisco DX Series devices include USB ports, and sometimes a micro-USB port. The devices support connection of a maximum of ten accessories to the USB ports. Each accessory that connects to the devices is included in

the maximum count. Supported accessories include USB serial cable, USB mouse, USB keyboard, USB-powered hub, and USB memory stick.

Note Because all USB hubs need to be powered, keyboards that include one or more hubs are not allowed on these devices, because they contain a nonpowered hub.

You can also use a USB connection for Android Debug Bridge (ADB) access. Use the micro-USB ports on Cisco DX650, and Cisco DX70, and the USB type B port on Cisco DX80 for ADB access. For more information about using ADB, see http://developer.android.com/index.html.

The USB Serial Console allows a USB port to be used as a console, thus eliminating the need for a serial port. The following table shows the settings for the USB console.

Table 7: USB Console Settings

Parameter	Setting
Baud rate	115200
Data	8 bit
Parity	none
Stop	1 bit
Flow control	none

Note Because the device comes preloaded with drivers, Cisco supports only a limited number of cable types. Cisco recommends use of the IOGEAR USB-serial adapter.

Use USB Console

The USB console cable has a USB interface on one end and a serial interface on the other. The USB interface may be plugged in to any of the USB ports on the device. The serial interface connects to the serial port on the PC.

For Cisco DX650, use either the side or rear USB type A port. For Cisco DX70 and Cisco DX80 use the micro-USB port.

Tip If you do not have a serial port on your PC/laptop, two USB console cables can be connected back to back, with a null modem cable between them.

Procedure

Step 1 In Cisco Unified Communications Manager, set credentials on the device page.
Step 2 Enable USB debugging in the Product Specific Configuration Layout portion of the window.
Step 3 Connect a USB serial cable to the device. The device console output appears on your terminal screen.
Step 4 After output stops, tap **Return** to sign in.
Step 5 After $ prompt screen, you can use tools such as debugsh to diagnose problems.

Behavior During Times of Network Congestion

Anything that degrades network performance can affect 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

To reduce or eliminate any adverse effects, schedule administrative network tasks during a time when the devices are not being used or exclude the devices from testing.