Configure Security, Quality, and Network Features

This chapter describes how to configure security, voice quality, and optional network features for the phone:

Set Security Features

The security features ensure that calls are secure and authenticated.

Configure Domain and Internet Settings

Configure Restricted Access Domains

If you enter domains, the Cisco IP phones respond to SIP messages only from the identified servers.

To configure restricted access domains, navigate to **Admin Login > advanced > Voice > System**. Under **System Configuration** in the Restricted Access Domains field. Enter fully-qualified domain names (FQDNs) for each SIP server you want the phone to respond to. Separate FQDNs with semicolons. For example, `voiceip.com;voiceip1.com`.

Configure DHCP and Static IP Connection Type

You can set the connection type to one of the following:

- Dynamic Host Configuration Protocol (DHCP) receives an IP address from the network DHCP server. The IP conference phones typically operate in a network where a DHCP server assigns the devices their IP addresses. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses its IP address for any reason, or if some other device on the network is assigned its IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the

DHCP Timeout on Renewal parameter causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.

- Static IP—A static IP address for the phone.

To set the connection type, navigate to **Admin Login > advanced > Voice > System**. Under **Internet Connection Type** choose the Connection Type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP, and configure the following:
  - **Static IP Address** of the phone.
  - **Netmask** of the phone.
  - **Gateway** IP address

DHCP Option Support

The table shows the DHCP options that are supported on the conference phones:

Network Standard	
DHCP option 1	Subnet mask
DHCP option 2	Time Offset
DHCP option 3	Router
DHCP option 6	Domain name server
DHCP option 15	Domain name
DHCP option 41	IP address lease time
DHCP option 42	NTP Server
DHCP option 43	Vendor Specific Information
DHCP option 60	Vendor class identifier
DHCP option 66	TFTP server name
DHCP option 125	Vendor-Identifying Vendor-Specific Information
DHCP option 150	TFTP server
DHCP option 158	
DHCP option 159	
DHCP option 160	

Challenge SIP Initial INVITE Messages

The SIP INVITE (initial) message in a session can be challenged by the endpoint. The challenge restricts the SIP servers that are permitted to interact with the devices on a service provider network. This significantly increases the security of the VoIP network by preventing malicious attacks against the device.

To configure SIP INVITE challenge, navigate to **Admin Login > advanced > Voice > Extension**. Under **SIP Settings** in the Auth INVITE field, choose **Yes**.

Encrypt Signaling with SIP Over TLS

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP Over TLS encrypts the SIP messages between the service provider SIP proxy and the end user. SIP Over TLS encrypts only the signaling messages, not the media.

TLS has two layers:

- TLS Record Protocol--layered on a reliable transport protocol, such as SIP or TCH, it ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable.
- TLS Handshake Protocol--authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

The IP conference phone uses UDP as a standard for SIP transport, but they also support SIP over TLS for added security.

To enable TLS for the phone, navigate to **Admin Login > advanced > Voice > Extension**. Under **SIP Settings**, select **TLS** from the SIP Transport list.

Configure Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. If the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G729a resource is already allocated (and since only one G.729a resource is allowed per IP phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Negotiation of the optimal voice codec sometimes depends on the ability of the conference phone to match a codec name with the far-end device or gateway codec name. The phone allows the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

Note that the conference phone supports voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec used for each line. G.711a and G.711u are always enabled.

To configure the voice codecs on each extension, navigate to **Admin Login > advanced > Voice > Extension**. Under **Audio Configuration**, configure the following parameters:

Parameter	Description
Preferred Codec	Preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: • G711u • G711a • G729a • G729ab • G722 • iLBC Defaults to G711u.
Use Pref Codec Only	To use only the preferred codecs for all calls, select **Yes**. (The call fails if the far end does not support these codecs.) Otherwise, select **No**. Defaults to No.
Second Preferred Codec	If the first codec fails, this codec is tried. Defaults to **unspecified**.
Third Preferred Codec	If the second codec fails, this codec is tried. Defaults to **unspecified**.
G711u Enable	Enables use of the G.711u codec. Defaults to Yes.
G711a Enable	Enables use of the G.711a codec. Defaults to Yes.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select **Yes**. Otherwise, select **No**. Defaults to Yes.
G722 Enable	Enables use of the G.722 codec. Defaults to Yes.
iLBC Enable	Enables use of the iLBC codec. Defaults to Yes.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **Yes**. Otherwise, select **No**. Defaults to No.
DTMF Tx Method	The method for transmitting DTMF signals to the far end. The options are: InBand, audio video transport (AVT), INFO, Auto, InBand+INFO, or AVT+INFO. • InBand sends DTMF by using the audio path. • AVT sends DTMF as AVT events. • INFO uses the SIP INFO method. • Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.

Set Optional Network Servers

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery.

To configure the (PoE) requirements, navigate to **Admin Login > advanced > Voice > System.** Under **Optional Network Configuration** configure the following fields:

- Host Name—The host name of the phone.
- Domain—The network domain of the phone. If using LDAP see the "Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control" section on page 2-7.
- Primary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0. If using LDAP see the "Configure LDAP for the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control" section on page 2-7.
- Secondary DNS—DNS server used by the phone in addition to the DHCP-supplied DNS servers (if DHCP is enabled), When DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.
- Syslog Server—Syslog server name and port for logging system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
- Debug Level—The debug level ranges from 0 to 3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
- Primary NTP Server—IP address or name of the primary NTP server used to synchronize its time. Defaults to blank.
- Secondary NTP Server—IP address or name of the secondary NTP server used to synchronize its time. Defaults to blank.
- DNS Cache TTL Ignore—When set to Yes, the DNS query results are not cached. When set to No, the phone will cache the A/AAAA/SRV/CNAME record according to the TTL responses. Defaults to Yes.
- SSH Access— The administrator can be configure this parameter to control the SSH console. Defaults to No.
- SSH User ID—The administrator can set the User ID for SSH login. Defaults to blank.
- SSH Password—The administrator can set the Password for SSH login. Defaults to blank.

Configure VLAN Settings

If you use a VLAN, your phone voice packets are tagged with the VLAN ID.

Configure Cisco Discovery Protocol (CDP)

CDP is negotiation-based and determines which VLAN the IP phone resides in. If you are using a Cisco switch, Cisco discovery protocol (CDP) is available and is enabled by default. CDP:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the IP conference phone.

Configure LLDP-MED

The IP conference phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other third-party network connectivity devices that use a Layer 2 auto-discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

The IP conference phone operates as LLDP-MED Media End Point Class III devices with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

The IP conference phone supports only the following limited set of TLVs as LLDP-MED Media Endpoint device class III:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- Port Description TLV
- System Name TLV
- System Capabilities TLV
- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)
- LLDP-MED Firmware Revision TLV
- End of LLDPDU TLV

The outgoing LLDPDU contains all the above TLVs when if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- End of LLDPDU TLV

The phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information is not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- There is no full validation of all TLVs; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are only used for reference.

TLV Information

These sections provide the TLV information.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports sub-type=5 (Network Address). When IP address is known, the value of Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for Chassis ID is `0.0.0.0`. The only INAN address family supported is IPv4. Currently, IPv6 address for the Chassis ID is not supported. For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form MSAP identifier. The value is not validated against its sub-type. The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

Port ID TLV

For the outgoing LLDPDU, the TLV supports sub-type=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID in wired or wireless mode. For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its sub-type. The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDUs.

Time to Live TLV

For the outgoing LLDPDU, the Time to live TTL value is 180 seconds. This is different from 120 seconds as recommended by the standard. For the shutdown LLDPDU, the TTL value is always 0. The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDUs.

End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs.

Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as “Port ID TLV” for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDUs.

System Name TLV

For the Cisco Unified IP Conference Phone 8831 for Third-Party Call Control, the value is SEP+MAC address.

Example: SEPAC44F211B1D0

The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDUs.

System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities field should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field. For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type. The System Capabilities TLV is mandatory for outgoing LLDPDUs. Only one System Capabilities TLV is allowed.

Management Address TLV

The TLV identifies an address associated with the local LLDP agent (that may be used to reach higher layer entities) to assist discovery by network management. The TLV allows the inclusion of both the system interface number and an object identifier (OID) that are associated with this management address, if either or both are known.

TLV information string length—This field contains the length (in octets) of all the fields in the TLV information string.

Management address string length—This field contains the length (in octets) of the management address subtype + management address fields.

System Description TLV

The TLV allows the network management to advertise the system's description.

TLV information string length—This field indicates the exact length (in octets) of the system description.

System description—This field contains an alpha-numeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system's hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.

IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for auto-negotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value auto-negotiation support/status should be:

- Bit 0—Set to 1 to indicate the auto-negotiation support feature is supported.
- Bit 1—Set to 1 to indicate auto-negotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD auto-negotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode
- Bit 14—10BASE-T full duplex mode
- Bit 11—100BASE-TX half duplex mode

- Bit 10—100BASE-TX full duplex mode
- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex
- 15—100BASE-TX half duplex
- 11—10BASE-T full duplex
- 10—10BASE-T half duplex

For example, in most cases, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone will send out this TLV only when in wired mode. When the phone is not set for auto-negotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value auto-negotiation support/status should be clear (0) to indicate auto-negotiation is disabled. The 2 octets PMD auto-negotiation advertised capability field should be set to 0x8000 to indicate unknown.

LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) and with the following bits set for 2-octet Capability field:

Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

Network Policy TLV

Outgoing LLDPDU—Before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

Incoming LLDPDU—Multiple Network Policy TLVs for different application types are allowed.

LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to “0 1” to indicate the power type for phone is PD Device. The Power source for the phone is set “PSE and local” with binary value “1 1”. The Power Priority is set to binary “0 0 0 0” to indicate unknown priority while the Power Value is set to maximum power value. The Power Value for the conference phone is 12900mW.

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the firmware revision is the firmware version. For the incoming LLDPDU, the TLVs are all ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS For the Phone

The following sections describe network policy and QoS for the IP phones.

Special VLANs

VLAN=0, VLAN=1 and VLAN=4095 are treated the same way as an untagged VLAN. As the VLAN is untagged, CoS is not applicable.

Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. ToS is based on configuration for the specific extension.

Default QoS for SPCP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on a predefined value of 5. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. ToS is based on configuration for the specific extension.

QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1 or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.
- If the VLAN > 1 and VLAN< 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.
- The phone reboots and restarts the fast start sequence.

QoS Resolution for LLDP-MED

If CoS is applicable and if CoS=0, the default will be used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on value used for extension 1. If CoS is applicable and if CoS != 0, CoS will be used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP=0, the default will be used for the specific extension as previously described. But the value show on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP != 0, DSCP will be used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS) and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for voice application from LLDP-MED PDU and if the tagged flag is not set, only the DPSC (mapped to ToS) is applicable.

The conference phone reboots and restarts the fast start sequence.

Co-Existence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN is determined by the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup, the phone sends both CDP and LLDP-MED PDUs at the same time.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set via CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN will be supported. DSCP is used and the network policy is determined by LLDP-MED if applicable.

LLDP-MED and Multiple Network Devices

If the same application type is used for network policy but different Layer 2 or Layer 3 QoS Network policies are received by the phones from multiple network connectivity devices, the last valid network policy is honored. To ensure deterministic and consistent of Network Policy, multiple network connectivity devices should not send out conflicting network policies for the same application type.

LLDP-MED and IEEE 802.X

The phones do not support IEEE 802.X and will not work in a 802.1X wired environment. However, IEEE 802.1X or Spanning Tree Protocols on network devices could result in delay of fast start response from switches.

Configure the VLAN Settings

To configure VLAN settings, navigate to **Admin Login > advanced > Voice > System**. Under **VLAN Settings**, configure the following parameters:

Parameter	Description
VLAN ID	If you use a VLAN without Cisco Discovery Protocol (CDP) (VLAN enabled and CDP disabled), enter a *VLAN ID* for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use **1** for the VLAN ID.
Enable CDP	Enable CDP only if you are using a switch that has CDP. CDP is negotiation-based and determines on which VLAN the IP phone resides.
Enable LLDP-MED	Choose **Yes** to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. (By default, this setting is enabled.) When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN is used if applicable. If CDP is used concurrently, a waiting period of 6 seconds is used. The waiting period increases the overall startup time for the phone.
Network Startup Delay	Enter the delay in seconds for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, it might be necessary to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.