Technical Details

Network Protocols

Cisco IP Phone 8800 Series support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the phones support.

Table 1: Supported Network Protocols on the Cisco IP Phone 8800 Series

Network protocol	Purpose	Usage notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	Cisco IP Phones 8845, 8865, and 8851 support Bluetooth 4.1. Cisco IP Phone 8861 support Bluetooth 4.0. Cisco IP Phone 8811 and 8841 do not support Bluetooth.
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco IP Phone, to discover certain startup information, such as the IP address.	—
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 Cisco IP Phones use 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.

Network protocol	Purpose	Usage notes
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 the phone to 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, and gateway on each phone locally. **Note** The **DHCP Option To Use** parameter has 66,160,159,150,60,43,125 as its default value. This value indicates the order in which the phone uses the IP address provided by the DHCP server.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco IP Phones use the HTTP protocol for XML services, provisioning the phone, upgrading the phone, 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.	Some Web applications support both HTTP and HTTPS protocols. Cisco IP Phones that support HTTPS use the HTTPS URL.
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 IP Phone implements 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 phone, you should disable the PC port and voice VLAN.
IEEE 802.11n/802.11ac	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11n operates at the 2.4 GHz and 5 GHz band and 802.11ac operates at the 5 GHz band.	The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable. Only Cisco IP Phone 8861 and 8865 support WLAN.

Network protocol	Purpose	Usage notes
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 gateway identifications are automatically assigned if you are using the Cisco IPPhone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
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 IPPhone supports LLDP on the PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard for voice products.	The Cisco IPPhone 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_paper0900aecd804cdd1.html
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice, over data networks.	Cisco IP 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 disabled 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 detection, and comfort noise, are normally configured on a global basis by Third-Party Call Control System 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. Cisco IP Phones support the SIP protocol when the phones are operating in IPv6-only, IPv4-only, or in both IPv4 and IPv6.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco IP Phones use TCP to connect to Third-Party Call Control system and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security implementation, Cisco IP Phones use the TLS protocol when securely registering with Third-Party Call Control system.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco IPPhone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify.
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 phones do not support UDP.

VLAN Interaction

The Cisco IP Phone contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (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 that connect to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP 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 to which the phone connects would be configured for 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 that connects to the switch through the computer (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 that does not have enough IP addresses for each phone.

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

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

USB Port Information

The Cisco IP Phones 8851, 8861, and 8865 support a maximum of five devices that connect to each USB port. Each device that connects to the phone is included in the maximum device count. For example, your phone can support five USB devices on the side port and five more standard USB devices on the back port. Many third-party USB products count as multiple USB devices; for example, a device containing a USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Note

- Unpowered hubs are not supported, and powered hubs with more than four ports are not supported.
- USB headsets that connect to the phone through a USB hub are not supported.

Each key expansion module connects to the phone counts as a USB device. If three key expansion modules are connected to the phone, these count as three USB devices.

Disable the USB Port

If you don't allow the users to use a or all USB ports for certain purposes, you can disable the back or the side, or both USB ports on the phone. The disabled USB port doesn't provide any function. For example, it doesn't recognize the USB headset and Key Expansion Module (KEM). Also, it doesn't charge any connected device.

The Cisco IP Phone 8851 contains only one USB port, the side USB port. The Cisco IP Phone 8861 and 8865 contain two USB ports, one side USB port and one back USB port.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **System**.

Step 2 Under the **Power Settings** section, set the parameter **Disable Back USB Port** to **Yes** to turn off the back USB port.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Disable_Back_USB_Port ua="na">No</Disable_Back_USB_Port>
```

Options: Yes and No

Default: No

Step 3 Under the **Power Settings** section, set the parameter **Disable Side USB Port** to **Yes** to turn off the side USB port.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Disable_Side_USB_Port ua="na">No</Disable_Side_USB_Port>
```

Options: Yes and No

Default: No

Step 4 Click **Submit All Changes**.

SIP and NAT Configuration

SIP and the Cisco IP Phone

The Cisco IP Phone uses Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving phone is called the SIP user agent server (UAS), while the requesting phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two UAs connect using a direct peer-to-peer session. Voice traffic transmits between UAs over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

SIP Over TCP

To guarantee state-oriented communications, the Cisco IP Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem of UDP port-blocking by corporate firewalls. With TCP, new ports do not need to be open or packets dropped, because TCP is already in use for basic activities, such as internet browsing or e-commerce.

SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. The phone supports the use of backup servers to minimize or eliminate service disruption.

A simple way to support proxy redundancy is to specify a SIP Proxy Server in the phone configuration profile. The phone sends a DNS NAPTR or SRV query to the DNS server. If configured, the DNS server returns SRV records that contain a list of servers for the domain, with their hostnames, priority, listening ports, and so forth. The phone tries to contact the servers in the order of the priority. The server with a lower number has a higher priority. Up to six NAPTR records and twelve SRV records are supported in a query.

When the phone fails to communicate with the primary server, the phone can failover to a lower-priority server. If configured, the phone can restore the connection back to the primary. Failover and failback support switches between servers with different SIP transport protocols. The phone doesn't perform failback to the primary server during an active call until the call ends and the failback conditions are met.

Example of Resource Records from the DNS Server

```
as1bsoft     3600    IN NAPTR 50   50  "s"  "SIPS+D2T"     ""  _sips._tcp.tlstest
             3600    IN NAPTR 90   50  "s"  "SIP+D2T"      ""  _sip._tcp.tcptest
             3600    IN NAPTR 100  50  "s"  "SIP+D2U"      ""  _sip._udp.udptest

_sips._tcp.tlstest  SRV 1 10 5061 srv1.sipurash.com.
                    SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest   SRV 1 10 5061 srv3.sipurash.com.
                    SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest   SRV 1 10 5061 srv5.sipurash.com.
                    SRV 2 10 5060 srv6.sipurash.com.

srv1     3600    IN    A   1.1.1.1
srv2     3600    IN    A   2.2.2.2
srv3     3600    IN    A   3.3.3.3
srv4     3600    IN    A   4.4.4.4
srv5     3600    IN    A   5.5.5.5
srv6     3600    IN    A   6.6.6.6
```

The following example shows the priority of the servers from the perspective of the phone.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS           UP
2nd            2.2.2.2            TLS           UP
3rd            3.3.3.3            TCP           UP
4th            4.4.4.4            TCP           UP
5th            5.5.5.5            UDP           UP
6th            6.6.6.6            UDP           UP
```

The phone always sends SIP messages to the available address with the top priority and with the status UP in the list. In the example, the phone sends all the SIP messages to the address 1.1.1.1. If the address 1.1.1.1 in the list is marked with the status DOWN, the phone communicates with 2.2.2.2 instead. The phone can restore the connection back to 1.1.1.1 when the specified failback conditions are met. For more details about failover and failback, see SIP Proxy Failover, on page 8 and SIP Proxy Fallback, on page 9.

SIP Proxy Failover

The phone performs a failover in any of these cases:

- The phone sends SIP messages and doesn't get responses from the server.
- The server responds with a code that matches the specified code in **Try Backup RSC**.
- The phone gets a TCP disconnection request.

We strongly recommend that you set the **Auto Register When Failover** to **Yes** when **SIP Transport** is set to **Auto**.

You can also configure this extension-specific parameters in the configuration file:

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

```
<Auto_Register_When_Failover_n_ ua="na">Yes</Auto_Register_When_Failover_n_>
```

where *n* is the extension number.

Phone Failover Behavior

When the phone fails to communicate with the currently connected server, it refreshes the server list status. The unavailable server is marked with the status DOWN in the server list. The phone tries to connect to the top-priority server with the status UP in the list.

In the following example, the addresses 1.1.1.1 and 2.2.2.2 aren’t available. The phone sends SIP messages to 3.3.3.3, which has the top priority among the servers with the status UP.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

In the following example, there are two SRV records from the DNS NAPTR response. For each SRV record, there are three A records (IP addresses).

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

Let's assume that the phone failed to connect to 1.1.1.1 and then registered to 1.1.1.2. When 1.1.1.2 goes down, phone behavior depends on the setting of **Proxy Fallback Intvl**.

- When **Proxy Fallback Intvl** is set to **0**, the phone tries with the addresses in this order: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- When **Proxy Fallback Intvl** is set to a value other than zero, the phone tries with the addresses in this order: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP Proxy Fallback

The proxy fallback requires a value other than zero specified in the **Proxy Fallback Intvl** field on the **Ext (n)** tab in the phone web interface. If you set this field to 0, the SIP proxy failback feature is disabled. You can also configure this extension-specific parameter in the configuration file in this format:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
```

where *n* is the extension number.

The time when the phone triggers a failback depends on the phone configuration and the SIP transport protocols in use.

To enable the phone to perform failback between different SIP transport protocols, set **SIP Transport** to **Auto** on the **Ext (n)** tab in the phone web interface. You can also configure this extension-specific parameter in the configuration file with the following XML string:

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

where *n* is the extension number.

Failback from a UDP Connection

The failback from a UDP connection is triggered by SIP messages. In the following example, the phone first failed to register to 1.1.1.1 (TLS) at the time T1 since there's no response from the server. When SIP Timer F expires, the phone registers to 2.2.2.2 (UDP) at the time T2 (T2=T1+SIP Timer F). The current connection is on 2.2.2.2 via UDP.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS          DOWN        T1 (Down time)
2nd            2.2.2.2            UDP          UP
3rd            3.3.3.3            TCP          UP
```

The phone has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The phone refreshes the registration at time T2 (T2=(3600-16)*78%). The phone checks the address list for the availability of the IP addresses and the down time. If T2-T1 > = 60, the failed server 1.1.1.1 resumes back to UP and the list is updated to the following. The phone sends SIP messages to 1.1.1.1.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS           UP
2nd            2.2.2.2            UDP           UP
3rd            3.3.3.3            TCP           UP
```

Failback from a TCP or TLS Connection

The failback from a TCP or TLS connection is triggered by the parameter **Proxy Fallback Intvl**. In the following example, the phone failed to register to 1.1.1.1 (UDP) at the time T1 and thus registered to 2.2.2.2 (TCP). The current connection is on 2.2.2.2 via TCP.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            UDP          DOWN        T1 (Down time)
2nd            2.2.2.2            TCP          UP
3rd            3.3.3.3            TLS          UP
```

The phone has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The proxy fallback interval (60 seconds) counts down from T1. The phone triggers proxy failback at the time of T1+60. If you set the proxy fallback interval to 0 in this example, the phone keeps the connection on 2.2.2.2.

Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages through primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone attempts to connect with the alternate proxy. If the phone fails to register to the primary proxy, it sends an INVITE to the alternate proxy without trying the primary proxy.

Dual registration is supported on a per-line basis. Three added parameters can be configured through web user interface and remote provisioning:

- Alternate Proxy—Default is empty.
- Alternate Outbound Proxy—Default is empty.
- Dual Registration—Default is NO (turned off).

After you configure the parameters, reboot the phone for the feature to take effect.

Note Specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

Dual Registration and DNS SRV Limitations

- When Dual Registration is enabled, DNS SRV Proxy Fallback or Recovery must be disabled.
- Do not use Dual Registration along with other Fallback or Recovery mechanisms. For example: Broadsoft mechanism.
- There is no recovery mechanism for feature request. However, the administrator can adjust the reregistration time for a prompt update of the registration state for primary and alternate proxy.

Dual Registration and Alternate Proxy

When the Dual Register parameter is set to **No**, Alternate Proxy is ignored.

Failover and Recovery Registration

- Failover—The phone performs a failover when transport timeout/failure or TCP connection failures; if Try Backup RSC and Retry Reg RSC values are datafilled.
- Recovery—The phone attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

  Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the phone re-registers upon failover or recovery.

Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

RFC3311

The Cisco IP Phone supports RFC-3311, the SIP UPDATE Method.

SIP NOTIFY XML-Service

The Cisco IP Phone supports the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is negotiation-based and determines which virtual LAN (VLAN) the Cisco IP Phone resides in. If you are using a Cisco switch, Cisco Discovery Protocol (CDP) is available and is enabled by default. CDP has these attributes:

- 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 Cisco IP Phone.

LLDP-MED

The Cisco IP Phone supports 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 Cisco IP Phone operates as a LLDP-MED Media End Point Class III device 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 Cisco IP Phone supports only the following limited set of Type-Length-Values (TLV) as an 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 preceding TLVs 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 Cisco IP 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 are not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- Full validation of all TLVs does not take place; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are used only for reference.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports subtype=5 (Network Address). When the IP address is known, the value of the 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 the Chassis ID is `0.0.0.0`. The only INAN address family supported is IPv4. Currently, the IPv6 address for the Chassis ID is not supported.

For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

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 subtype=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID.

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 subtype.

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 differs from the 120-second value that the standard recommends. 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 IP Phone, 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 fields 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 description.

- TLV information string length—This field indicates the exact length (in octets) of the system description.
- System description—This field contains an alphanumeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system 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 autonegotiation, 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 autonegotiation support/status should be:

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

The bit values for the 2 octets PMD autonegotiation 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, usually, 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 sends out this TLV only when in wired mode. When the phone is not set for autonegotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value autonegotiation support/status should be clear (0) to indicate that autonegotiation is disabled. The 2 octets PMD autonegotiation 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) 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

In the TLV for the 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.

In the TLV for the 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 to “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 Cisco IP 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 the 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 version of firmware on the phone. For the incoming LLDPDU, the TLVs are ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS

Special VLANs

VLAN=0, VLAN=1, and VLAN=4095 are treated the same way as an untagged VLAN. Because the VLAN is untagged, Class of Service (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. Type of Service (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 is used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on the value used for extension 1. If CoS is applicable and if CoS != 0, CoS is used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP = 0, the default is 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 is 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 the 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 the voice application from LLDP-MED PDU and if the tagged flag is not set, only the DSCP (mapped to ToS) is applicable.

The Cisco IP Phone reboots and restarts the fast start sequence.

Coexistence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN determines 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 CDP and LLDP-MED PDUs.

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

LLDP-MED and Multiple Network Devices

If the same application type is used for the 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 Cisco IP Phone does not support IEEE 802.X and does 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.