技术详情

网络协议

Cisco 8800 系列 IP 电话支持进行语音通信所需的多个行业标准及 Cisco 网络协议。下表列出了电话支持的网络协议。

表 *1: Cisco 8800* 系列 *IP* 电话支持的网络协议

网络协议	目的	使用注意事项
蓝牙	蓝牙是一种无线个人局域网 (WPAN) 协议，指定设备如何在短距离内通信。	Cisco 8845、8865 和 8851 IP 电话支持蓝牙 4.1。 Cisco 8861 IP 电话支持蓝牙 4.0。 Cisco 8811 和 8841 IP 电话不支持蓝牙。
Bootstrap 协议 (BootP)	BootP 支持网络设备（例如 Cisco IP 电话）发现特定的启动信息（例如 IP 地址）。	—
Cisco Discovery Protocol (CDP)	CDP 是用于发现设备的协议，在 Cisco 制造的设备上运行。 通过 CDP，设备可以向其他设备播发其存在，并收到关于网络中其他设备的信息。	Cisco IP 电话使用 CDP 向 Cisco Catalyst 交换机传达辅助 VLAN ID、每端口电源管理详情和服务质量 (QoS) 配置信息等信息。

技术详情

网络协议	目的	使用注意事项
动态主机配置协议 (DHCP)	DHCP 动态分配和指定网络设备的 IP 地址。 通过 DHCP，您可以将 IP 电话连接到网络中使电话可以运行，且无需手动分配 IP 地址或配置额外的网络参数。	默认情况下启用 DHCP。如果禁用，您必须在每部电话上本地手动配置 IP 地址、子网掩码和网关。 注释 **要使用的 DHCP 选项**参数具有 66,160,159,150,60,43,125 作为其默认值。该值指示电话使用 DHCP 服务器提供的 IP 地址的顺序。
超文本传输协议 (HTTP)	HTTP 是在 Internet 及 Web 上传输信息和移动文档的标准方式。	Cisco IP 电话使用 HTTP 协议提供 XML 服务、部署电话、升级电话以及进行故障排除。
安全超文本传输协议 (HTTPS)	安全超文本传输协议 (HTTPS) 将超文本传输协议与 SSL/TLS 协议组合到一起，提供服务器的加密和安全识别。	某些 Web 应用程序同时支持 HTTP 和 HTTPS 协议。支持 HTTPS 的 Cisco IP 电话使用 HTTPS URL。
IEEE 802.1X	IEEE 802.1X 标准定义了基于客户端-服务器的访问控制以及限制未经授权的客户端通过公开访问的端口连接到 LAN 的验证协议。 客户端通过验证之前，802.1X 访问控制只允许通过 LAN 的可扩展验证协议 (EAPOL) 流量流经客户端所连端口。成功通过验证后，常规流量才能流经该端口。	Cisco IP 电话通过支持下列验证方法实施 IEEE 802.1X 标准：EAP-FAST 和 EAP-TLS。 在电话上启用 802.1X 验证时，应禁用 PC 端口和语音 VLAN。
IEEE 802.11n/802.11ac	IEEE 802.11 标准指定设备如何通过无线局域网 (WLAN) 进行通信。 802.11n 在 2,4 GHz 和 5 GHz 频段工作，而 802.11ac 在 5 GHz 频段工作。	802.11 接口是以太网接线不可用或不需要时的部署选项。 仅 Cisco 8861 和 8865 IP 电话支持 WLAN 功能。
Internet 协议 (IP)	IP 是在网络上寻址和发送信息包的消息传送协议。	要使用 IP 通信，网络设备必须分配有 IP 地址、子网和网关。 如果您使用的是支持动态主机配置协议 (DHCP) 的 Cisco IP 电话，系统会自动分配 IP 地址、子网和网关标识。如果您未使用 DHCP，则必须手动向每部电话分配上述属性。
链路层发现协议 (LLDP)	LLDP 是标准化的网络发现协议（类似于 CDP），部分 Cisco 和第三方设备支持该协议。	Cisco IP 电话的 PC 端口支持 LLDP。

技术详情

网络协议	目的	使用注意事项
链层发现协议-媒体终端设备 (LLDP-MED)	LLDP-MED 是针对语音产品的 LLDP 标准的延伸。	Cisco IP 电话的 SW 端口支持使用 LLDP-MED 发送下列信息： • 语音 VLAN 配置 • 设备发现 • 电源管理 • 库存管理 有关 LLDP-MED 支持的详细信息，请参阅 LLDP-MED 和 Cisco Discovery Protocol 白皮书，网址为： [illegible]
实时传输协议 (RTP)	RTP 是用于通过数据网络传输实时数据（例如交互式语音）的标准协议。	Cisco IP 电话使用 RTP 协议与其他电话和网关之间收发实时语音流量。
实时控制协议 (RTCP)	RTCP 与 RTP 配合使用时，可以在 RTP 流中提供 QoS 数据（例如抖动、延迟和往返延迟）。	默认情况下禁用 RTCP。
会话描述协议 (SDP)	SDP 是确定两个终端连接期间哪些参数可用的 SIP 协议。会议通过仅使用会议中所有终端支持的 SDP 功能建立。	编解码器类型、DTMF 检测和舒适噪音等 SDP 功能通常在全局基础上通过运行中的第三方呼叫控制系统或媒体网关进行配置。有些 SIP 终端可能允许在终端上自行配置这些参数。
会话发起协议 (SIP)	SIP 是用于通过 IP 召开多媒体会议的互联网工程任务组 (IETF) 标准。SIP 是基于 ASCII 的应用层控制协议（如 RFC 3261 中定义），可用于建立、维持和终止两个或更多终端之间的呼叫。	和其他 VoIP 协议类似，SIP 可在信息包电话网络中提供信令和会话管理功能。信令允许在网络边界上传输呼叫信息。会话管理能够控制端到端呼叫的属性。 电话在仅 IPv6、仅 IPv4 或者同时在 IPv4 和 IPv6 模式下运行时，Cisco IP 电话支持 SIP 协议。
传输控制协议 (TCP)	TCP 是一种面向连接的传输协议。	Cisco IP 电话使用 TCP 连接到第三方呼叫控制系统并访问 XML 服务。
传输层安全 (TLS)	TLS 是用于确保通信安全并对通信进行验证的标准协议。	实施安全性后，Cisco IP 电话安全地向第三方呼叫控制系统注册时使用 TLS 协议。
普通文件传输协议 (TFTP)	TFTP 允许您通过网络传输文件。 在 Cisco IP 电话上，通过 TFTP 可获取特定于电话类型的配置文件。	TFTP 要求网络中有 TFTP 服务器（DHCP 服务器可自动识别）。

网络协议	目的	使用注意事项
用户数据报协议 (UDP)	UDP 是用于传送信息包的无连接消息传送协议。	UDP 仅用于 RTP 流。电话上的 SIP 信令不支持 UDP。

VLAN 交互

Cisco IP 电话包含一个内部以太网交换机，可前转信息包至电话以及电话后端的计算机（接入）端口和网络端口。

如果计算机连接至计算机（访问）端口，计算机和电话将共享通向交换机的同一条物理链路并共享交换机上的同一端口。此共享物理链路对于网络上的 VLAN 配置具有以下含义：

- 当前 VLAN 可能基于 IP 子网配置。但其他 IP 地址可能不可用于将电话分配到连接相同端口的其他设备所在的子网。
- 在支持电话的 VLAN 上进行数据通信，可能降低 VoIP 通信质量。
- 网络安全可能显示有必要隔离 VLAN 语音通信和 VLAN 数据通信。

您可以通过将语音通信隔离到独立的 VLAN 上来解决这些问题。电话所连接的交换机端口可能会针对独立 VLAN 进行配置以承载：

- 往来 IP 电话（例如 Cisco Catalyst 6000 系列上的辅助 VLAN）的语音通信
- 往来 PC 的数据通信，该 PC 通过 IP 电话（本机 VLAN）的计算机（访问）端口连接到交换机

隔离电话到独立的辅助 VLAN 上，提高语音通信的质量并允许将大量电话添加到没有足够 IP 地址供每台电话使用的现有网络。

有关详细信息，请参阅思科交换机随附的文档。您还可以在以下 URL 访问交换机信息：

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

USB 端口信息

Cisco 8851、8861 和 8865 IP 电话最多支持五台设备连接到每个 USB 端口。 每个连接到电话的设备都计入最大设备计数。 例如，电话的侧面端口可支持五个 USB 设备，背面端口可再支持五个标准 USB 设备。 许多第三方 USB 产品被视为多个 USB 设备，例如，一个包含 USB 集线器和头戴式耳机的设备被视为两个 USB 设备。 有关详细信息，请参阅 USB 设备文档。

注释

- 非供电集线器不受支持，具有四个以上端口的供电集线器不受支持。
- 不支持通过 USB 集线器连接到电话的 USB 头戴式耳机。

连接到电话的每个按键扩展模块均计为一个USB设备。 如果有三个按键扩展模块连接到电话，则计为三个 USB 设备。

禁用 USB 端口

如果您不允许用户将一个或所有 USB 端口用于某些目的，您可以禁用电话的背面或侧面 USB 端口或两个 USB 端口。 禁用的 USB 端口不提供任何功能。 例如，它不能识别 USB 头戴式耳机和按键扩展模块 (KEM)。 此外，它不会为任何连接的设备充电。

Cisco IP Phone 8851 只包含一个 USB 端口，即侧面 USB 端口。 Cisco 8861 和 8865 IP 电话包含两个 USB 端口、一个侧面 USB 端口和一个背面 USB 端口。

开始之前

访问电话管理网页。 请参阅：访问电话 Web 界面。

过程

步骤 1 选择 **Voice** > **System**。

步骤 2 在**电源设置**部分，将参数**禁用背面 USB 端口**设置为**是**以关闭背面 USB 端口。

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

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

选项：Yes 和 No

默认值：No

步骤 3 在**电源设置**部分，将参数**禁用侧面 USB 端口**设置为**是**以关闭侧面 USB 端口。

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

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

选项：Yes 和 No

默认值：No

步骤 4 单击 **Submit All Changes**。

SIP 和 NAT 配置

SIP 和 Cisco IP 电话

Cisco IP 电话使用会话发起协议 (SIP)，该协议允许与支持 SIP 的所有 IT 服务提供商进行互操作。 SIP 是一种 IETF 定义的信令协议，该协议可控制 IP 网络中的语音通信会话。

SIP 处理数据包电话网络内的信令和会话管理。 信令允许跨网络边界传输呼叫信息。 会话管理控制端到端呼叫的属性。

在典型商业 IP 电话部署中，所有呼叫均会通过 SIP 代理服务器。 接收传入呼叫的电话称为 SIP 用户代理服务器 (UAS)，发出请求的电话则称为用户代理客户端 (UAC)。

SIP 消息路由是动态的路由。 如果 SIP 代理收到来自 UAS 的连接请求，但无法找到 UAC，代理会将消息前转到网络中的另一个 SIP 代理。 定位到 UAC 之后，响应会路由回 UAS，然后两个 UA 使用直接的对等会话进行连接。 语音流量使用实时传输协议 (RTP) 通过动态分配的端口在 UA 之间传输。

RTP 传输音频和视频等实时数据；RTP 不保证实时数据传输。 RTP 提供发送和接收应用程序的机制，以支持流数据。 一般而言，RTP 在 UDP 之上运行。

基于 TCP 的 SIP

为了确保面向状态的通信，Cisco IP 电话可以使用 TCP 作为 SIP 的传输协议 。 此协议能保障传输的可靠性，确保会重新传输丢失的数据包。 TCP 还可保证按照发送的顺序接收 SIP 数据包。

TCP 解决了企业防火墙阻止 UDP 端口的问题。 由于 TCP 已运用于网页浏览、电子商务等基本活动，因此新端口无需打开，也不需要丢弃数据包。

SIP 代理冗余

一个普通 SIP 代理服务器可以处理成千上万个订户。 有了备份服务器，就可以暂时关闭主服务器以对其进行维护。 电话支持使用备份服务器来最大程度减少或消除服务中断的情况。

要为代理冗余提供支持，一种简单的方法是在电话配置文件中指定 SIP 代理服务器。 电话向 DNS 服务器发送 DNS NAPTR 或 SRV 查询。 如果对 DNS 服务器进行了配置，它会返回一条包含域的服务器列表的 SRV 记录，其中列有服务器的主机名、优先级、侦听端口等。 电话会尝试按照优先级顺序与这些服务器联系。 编号越小，服务器的优先级越高。 查询中最多支持六条 NAPTR 记录和十二条 SRV 记录。

当电话无法与主服务器通信时，电话可以故障转移到优先级较低的服务器。 如果已配置，电话可恢复主服务器连接。 故障转移和故障恢复支持在使用不同 SIP 传输协议的服务器之间切换。 在通话过程中，电话不会执行到主服务器的故障恢复，除非呼叫结束且满足故障恢复条件。

DNS 服务器中的资源记录示例

```
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
```

以下示例显示了从电话角度来看，服务器的优先级。

```
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
```

电话始终会将 SIP 消息发送到列表中优先级最高且状态为 UP 的可用地址。 在本例中，电话会将所有 SIP 消息发送到地址 1.1.1.1。 如果列表中 1.1.1.1 的地址被标示为 DOWN，则电话将与 2.2.2.2 通信。 当满足指定的故障恢复条件时，电话可恢复到 1.1.1.1 的连接。 有关故障转移和故障恢复的更多详细信息，请参阅SIP 代理故障转移 ， 第 7 页和SIP 代理回退 ， 第 8 页。

SIP 代理故障转移

电话在以下任何情况下都会执行故障转移：

- 电话将发送 SIP 消息，且不会收到来自服务器的响应。
- 服务器将使用与**尝试备份 RSC** 中的指定代码匹配的代码作出响应 。
- 电话会收到 TCP 连接断开请求。

如果 **SIP 传输**设置为**自动**，我们强烈建议您将**故障转移时自动注册**设置为**是**。

您还可以在配置文件中配置这个特定于分机的参数：

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

其中 *n* 是分机号码。

电话故障转移行为

当电话无法与当前连接的服务器通信时，会刷新服务器列表状态。 在服务器列表中，不可用服务器的状态标示为 DOWN。 电话将尝试连接到列表中状态为 UP 的优先级最高的服务器。

在以下示例中，地址 1.1.1.1 和 2.2.2.2 不可用。 电话会将 SIP 消息发送到 3.3.3.3，在状态为 UP 的服务器中，其优先级最高。

```
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
```

在下面的示例中，DNS NAPTR 响应中有两条 SRV 记录。 对于每条 SRV 记录，都有三个 A 记录（IP 地址）。

```
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
```

假设电话未能连接到 1.1.1.1，然后注册到 1.1.1.2。 当 1.1.1.2 发生故障时，电话行为取决于 **Proxy Fallback Intvl** 的设置。

- 当 **Proxy Fallback Intvl** 设置为 **0** 时，电话将按以下顺序尝试连接地址：1.1.1.1、1.1.1.3、2.2.2.1、2.2.2.2、2.2.2.3。
- 当**代理回退间隔时间**设置为非零的值时，电话将按以下顺序尝试连接地址：1.1.1.3、2.2.2.1、2.2.2.2、2.2.2.3。

SIP 代理回退

要使用代理回退，必须在电话 Web 界面**分机 (n)** 选项卡的**代理回退间隔时间**字段中指定非零的值。 如果此字段设置为 0，SIP 代理故障恢复功能将禁用。 您还可以在配置文件中按照以下格式配置这个特定于分机的参数：

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

其中 *n* 是分机号码。

电话触发故障恢复的时间取决于所使用的电话配置和 SIP 传输协议。

要让电话在不同 SIP 传输协议之间执行故障恢复，请在电话 Web 界面的**分机 (n)** 选项卡上将 **SIP 传输**设置为**自动**。 您还可以在配置文件中利用以下 XML 字符串配置这个特定于分机的参数：

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

其中 *n* 是分机号码。

从 UDP 连接执行故障恢复

从 UDP 连接执行故障恢复由 SIP 消息触发。 在以下示例中，由于服务器没有响应，电话第一次在 T1 时间未能注册到 1.1.1.1 (TLS)。 SIP 计时器 F 到期后，电话将在 T2 时间（T2 = T1 + SIP 计时器 F）注册到 2.2.2.2 (UDP)。 当前连接是在 2.2.2.2 上通过 UDP 完成的。

```
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
```

电话的配置如下：

```
<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>
```

其中 *n* 是分机号码。

电话将在 T2 时间 (T2=(3600-16)*78%) 刷新注册。 电话会检查地址列表，了解 IP 地址的可用性和停机时间。 如果 T2-T1 > = 60，失败的服务器 1.1.1.1 的状态将恢复为 UP，并且列表更新为如下所示。 电话将 SIP 消息发送到 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
```

从 TCP 或 TLS 连接执行故障恢复

从 TCP 或 TLS 连接执行故障恢复由**代理回退间隔时间**参数触发。 在以下示例中，电话在 T1 时间无法注册到 1.1.1.1 (UDP)，因此注册到 2.2.2.2 (TCP)。 当前连接是在 2.2.2.2 上通过 TCP 完成的。

```
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
```

电话的配置如下：

```
<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>
```

其中 *n* 是分机号码。

代理回退间隔时间（60 秒）从 T1 开始倒数。 电话会在 T1 + 60 时触发代理故障恢复。 如果在本例中将代理回退间隔时间设置为 0，则电话会在 2.2.2.2 上保持连接。

双重注册

电话始终同时注册到主（或主出站）代理和备用（或备用出站）代理。 注册后，电话会首先通过主代理发出邀请和非邀请 SIP 消息。 如果在新邀请超时后主代理没有响应，电话将尝试使用备用代理连接。 如果电话无法注册到主代理，它会向备用代理发送邀请，而不会尝试向主代理发送。

双重注册的受支持原则以线路为基础。 通过 web 用户界面和远程设置，可以配置三个附加的参数：

- 备用代理 — 默认值为空。
- 备用出站代理 — 默认值为空。
- 双重注册 — 默认值为否（关闭）。

配置参数后，重新启动电话以使功能生效。

Note 指定主代理（或主出站代理）和备用代理（或备用出站代理）的值以确保功能正常发挥作用。

双重注册和 DNS SRV 限制

- 当启用双重注册后，必须禁用 DNS SRV 代理回退或恢复。

- 不要将双重注册与其他回退或恢复机制一起使用。 例如：Broadsoft 机制。
- 没有适用于功能请求的恢复机制。 但是，管理员可以调整重新注册时间，以便提示更新主代理和备用代理的注册状态。

双重注册和备用代理

当双重注册参数设置为**无**时，备用代理将被忽略。

故障转移和恢复注册

- 故障转移 — 如果“尝试备份 RSC”和“重试注册 RSC”值已填入数据，当传输超时/失败或 TCP 连接失败时，电话会执行故障转移。
- 恢复 — 电话在注册或有效连接到辅代理的同时，尝试向主代理重新注册。

  出现错误时，如果故障转移参数控制故障转移行为，则自动注册。 当此参数设置为“是”时，电话在故障转移或恢复时会重新注册。

回退行为

当前注册过期或代理回退间隔触发时发生回退。

如果超出代理回退间隔的时间，所有新的 SIP 消息将转至主代理。

例如，当注册过期值为 3600 秒且代理回退间隔的时间为 600 秒，则在 600 秒后触发回退。

当注册过期值为 800 秒且代理回退间隔的时间为 1000 秒，则在 800 秒触发回退。

成功注册回主服务器后，所有的 SIP 消息将转到主服务器。

RFC3311

Cisco IP 电话支持 RFC 3311（SIP UPDATE 方法）。

SIP 通知 XML 服务

Cisco IP 电话支持 SIP 通知 XML 服务事件。 当收到含 XML 服务事件的 SIP 通知消息时，如果消息中无正确的凭证，电话质询通知时会收到 401 响应消息。 客户端必须提供采用 DIGEST-MD5 并含有 IP 电话相应线路的 SIP 帐户密码的正确凭证。

消息正文可以包含 XML 事件消息。 例如：

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

验证：

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

使用会话边界控制器进行 NAT 映射

我们建议您选择支持会话边界控制器 NAT 映射的服务提供商。 使用服务提供商提供的 NAT 映射，您在选择路由器时拥有更多的选择。

使用 SIP ALG 路由器进行 NAT 映射

使用具有 SIP 应用层网关 (ALG) 的路由器可以实现 NAT 映射。 通过使用 SIP ALG 路由器，您有多个服务提供商选项可选择。

Cisco Discovery Protocol

思科发现协议 (CDP) 经协商达成，并确定了 Cisco IP 电话所在的虚拟局域网 (VLAN)。如果使用的是思科交换机，则思科发现协议 (CDP) 可用且默认情况下处于启用状态。 CDP 具有以下特性：

- 获取相邻设备的协议地址，并发现这些设备的平台。
- 显示路由器所用接口的相关信息。
- 是媒体和协议无关。

如果您在不启动 CDP 的情况下使用 VLAN，必须为 Cisco IP 电话输入 VLAN ID。

LLDP-MED

部署与思科设备或其他使用第2层自动发现机制的第三方网络连接设备一起使用时，Cisco IP 电话支持媒体终端设备链路层发现协议 (LLDP-MED)。 根据 2005 年 5 月发布的 IEEE 802.1AB (LLDP) 规范和 2006 年 4 月发布的 ANSI TIA-1057 来实施 LLDP-MED。

根据媒体终端发现参考模型和定义（ANSI TIA-1057 第 6 部分），Cisco IP 电话作为 LLDP-MED 媒体终端第三类设备运行，与网络连接设备之间存在直接 LLDP-MED 链路。

作为 LLDP-MED 媒体终端第三类设备，Cisco IP 电话仅支持以下类型-长度-值 (TLV)：

- 机箱 ID TLV
- 端口 ID TLV
- 生存时间 TLV
- 端口说明 TLV
- 系统名称 TLV
- 系统功能 TLV
- IEEE 802.3 MAC/PHY 配置/状态 TLV（仅适用于有线网络）
- LLDP-MED 功能 TLV

- LLDP-MED 网络策略 TLV（仅适用于应用程序类型 = 语音）
- LLDP-MED 扩展 MDI 供电 TLV（仅适用于有线网络）
- LLDP-MED 固件版本 TLV
- LLDPDU 终止 TLV

如适用，发送 LLDPDU 包含上述所有 TLV。 对于传入呼叫 LLDPDU，如果以下任何一个 TLV 丢失，则丢弃 LLDPDU。 所有其他 TLV 将不会被验证，且会被忽略。

- 机箱 ID TLV
- 端口 ID TLV
- 生存时间 TLV
- LLDP-MED 功能 TLV
- LLDP-MED 网络策略 TLV（仅适用于应用程序类型 = 语音）
- LLDPDU 终止 TLV

如适用，Cisco IP 电话发出关闭 LLDPDU。 LLDPDU 帧包含以下 TLV：

- 机箱 ID TLV
- 端口 ID TLV
- 生存时间 TLV
- LLDPDU 终止 TLV

在 Cisco IP 电话上实施 LLDP-MED 会存在一些限制：

- 不支持存储和检索邻居的信息。
- 不支持 SNMP 和相应的 MIB。
- 不支持记录和检索统计计数器。
- 不会对所有 TLV 进行验证；不适用于电话的 TLV 将被忽略。
- 标准中所述的协议状态机仅供参考用。

机箱 ID TLV

对于去电 LLDPDU，TLV 支持子类型 = 5（网络地址）。 如果 IP 地址已知，则 Chassis ID 值由 INAN 地址族值的八位字节，加上随后的用于语音通信的 IPv4 地址的八位字节字符串组成。 如果 IP 地址未知，则 Chassis ID 值为 `0.0.0.0`。 唯一受支持的 INAN 地址族为 IPv4。 目前不支持 IPv6 地址用于 Chassis ID。

对于传入呼叫 LLDPDU，机箱 ID 将被视为形成 MSAP 标识符的不透明值。 不会根据子类型验证该值。

机箱 ID TLV 将强制作为首个 TLV。 仅允许一个机箱 ID TLV 用于去电和传入呼叫 LLDPDU。

端口 ID TLV

对于去电 LLDPDU，TLV 支持“子类型=3”（MAC 地址）。 端口 ID 的值使用的是以太网端口的 6 个八位字节 MAC 地址。

对于传入呼叫 LLDPDU，端口 ID TLV 将被视为形成 MSAP 标识符的不透明值。 不会根据子类型验证该值。

端口 ID TLV 是第二个强制性的 TLV。 仅允许一个端口 ID TLV 用于去电和传入呼叫 LLDPDU。

生存时间 TLV

对于去电 LLDPDU，生存时间 TTL 值为 180 秒。 这不同于 120 秒的标准建议值。 对于关闭 LLDPDU，TTL 值始终为 0。

作为第三个 TLV，生存时间 TLV 是必填项。 仅允许一个生存时间 TLV 用于去电和传入呼叫 LLDPDU。

LLDPDU 终止 TLV

该值为 2 个八位字节，均为 0。 该 TLV 为必填项，仅允许一个 TLV 用于去电和传入呼叫 LLDPDU。

端口说明 TLV

对于去电 LLDPDU，在端口说明 TLV 中，端口说明的值与 CDP 的“端口 ID TLV”相同。 对于传入呼叫 LLDPDU，端口说明 TLV 会被忽略且未经验证。 仅允许一个端口 ID TLV 用于去电和传入呼叫 LLDPDU。

系统名称 TLV

对于 Cisco IP 电话，值为 SEP+MAC 地址。

示例：SEPAC44F211B1D0

对于传入呼叫 LLDPDU，系统名称 TLV 会被忽略且未经验证。 仅允许一个系统名称 TLV 用于去电和传入呼叫 LLDPDU。

系统功能 TLV

对于系统功能 TLV 中的去电 LLDPDU，就带 PC 端口的电话而言，应将 2 个八位字节系统功能字段的位值分别设置为“2 位（桥）”和“5 位（电话）”。 如果电话没有 PC 端口，则只需设置 5 位。已启用的功能字段应设置为相同的系统功能值。

对于传入呼叫 LLDPDU，系统 TLV 将被忽略。 不会对照 MED 设备类型对 TLV 进行语义验证。

系统功能 TLV 对于去电 LLDPDU 是必需的。 仅允许存在一个系统功能 TLV。

管理地址 TLV

TLV 识别与本地 LLDP 代理相关联的地址（可用于到达更高层实体）以协助通过网络管理的发现。 TLV 允许包含与该管理地址相关联的系统接口号和对象标识符 (OID)（如果其中一个或两者都已知）。

- TLV信息字符串长度—此字段包含TLV信息字符串中所有字段的长度（以八位字节为单位）。
- 管理地址字符串长度 — 此字段包含管理地址子类型 + 管理地址字段的长度（以八位字节为单位）。

系统说明 TLV

TLV 允许进行网络管理以通告系统说明。

- TLV 信息字符串长度 — 此字段指示系统说明的实际长度（以八位字节为单位）。
- 系统说明 — 此字段包含作为网络实体文字说明的字母数字字符串。 系统说明包括系统硬件类型、软件操作系统和网络软件的全称和版本标识。 如果实施支持IETF RFC 3418，则应将sysDescr对象用于此字段。

IEEE 802.3 MAC/PHY 配置/状态 TLV

TLV 不用于自动协商，而是用于故障排除。 对于传入呼叫 LLDPDU，TLV 会被忽略且未经验证。 对于去电 LLDPDU，TLV 八位字节值的自动协商支持/状态应为：

- 0 位 — 设为 1，表示支持自动协商支持功能。
- 1 位 — 设为 1，表示已启用自动协商状态。
- 2-7 位 — 设为 0。

2 个八位字节的 PMD 自动协商功能字段的位值应设置为：

- 13 位 — 10BASE-T 半双工模式
- 14 位 — 10BASE-T 全双工模式
- 11 位 — 100BASE-TX 半双工模式
- 10 位 — 100BASE-TX 全双工模式
- 15 位 — 未知

应设置 10、11、13 和 14 位。

2 个八位字节工作 MAU 类型的设置值应反映工作 MAU 的实际类型：

- 16 — 100BASE-TX 全双工
- 15 — 100BASE-TX 半双工
- 11 — 10BASE-T 全双工
- 10 — 10BASE-T 半双工

例如，电话通常设置为 100BASE-TX 全双工。 然后应将值设为 16。 TLV 可用于有线网络，但不适用于无线网络。 仅在有线模式下，电话才会发送此 TLV。 如果电话未为去电 LLDPDU TLV 设置自动协商，但设置了特定快速/双工，八位字节值自动协商支持/状态的 1 位应清零 (0)，表示已禁用自动协商。 2 个八位字节 PMD 自动协商功能字段应设置为 0x8000，表示未知。

LLDP-MED 功能 TLV

对于去电 LLDPDU，TLV 应设有设备类型 3（第三类终端），以及下列为“功能”字段（长度为 2 个八位字节）设置的位：

位的位置	功能
0	LLDP-MED 功能
1	网络策略
4	通过 MDI-PD 扩展电源
5	清单

对于传入呼叫 TLV，如果 LLDP-MED TLV 不存在，LLDPDU 将被丢弃。 LLDP-MED 功能 TLV 为必须携带的 TLV，仅允许一个 TLV 用于去电和传入呼叫 LLDPDU。 在 LLDP-MED 功能 TLV 前显示的任何其他 LLDP-MED TLV 将被忽略。

网络策略 TLV

在去电 LLDPDU 的 TLV 中，在确定 VLAN 或 DSCP 之前，未知策略标志 (U) 设置为 1. 如果已知 VLAN 设置或 DSCP，则将该值设置为 0。当策略未知时，所有其他值都设置为 0。在确定或使用 VLAN 之前，标记标志 (t) 设置为 0。如果电话使用标记的 VLAN (VLAN ID > 1)，则标记标志 (t) 设置为 1. 保留 (x) 始终设置为 0。如果使用 VLAN，相应的 VLAN ID 和 L2 优先级将相应设置。 VLAN ID 有效值介于 1-4094 之间。 但是，永远不会使用 VLAN ID=1（限制）。 使用 DSCP 时，此值相应设置为介于 0-63 之间。

对于传入呼叫 LLDPDU 的 TLV，允许针对不同的应用类型使用多个网络策略 TLV。

LLDP-MED 通过 MDI 扩展电源 TLV

对于去电 LLDPDU 的 TLV，电源类型的二进制值设置为“0 1”表示电话的电源类型是 PD 设备。电话的电源设置为“PSE 和本地”，二进制值为“1 1”。 电源优先级设置为二进制值“0 0 0 0”表示电源值设置为最大电源值时优先级未知。 Cisco IP 电话的电源值为 12900mW。

对于传入呼叫LLDPDU，TLV会被忽略且未经验证。 去电和传入呼叫LLDPDU中仅允许一个TLV。 电话将仅发出有线网络的 TLV。

LLDP-MED 标准最初是针对以太网环境制定的。 针对无线网络的 LLDP-MED 目前正在商讨之中。 请参阅 ANSI-TIA 1057，附件 C，C.3 适用于 VOWLAN 的 TLV，表 24。建议 TLV 不应用于无线网络的上下文。 此 TLV 仅适用于 PoE 和以太网环境。 如果添加，TLV 不提供交换机处的任何网络管理或电源策略调整值。

LLDP-MED 清单管理 TLV

此 TLV 是第三类设备的可选项。 对于去电 LLDPDU，我们仅支持固件修订版本 TLV。 固件修订版本的值是电话固件的版本。 对于传入呼叫 LLDPDU，TLV 会被忽略且未经验证。 仅允许一个固件版本 TLV 用于去电和传入呼叫 LLDPDU。

最终网络策略解决方案和 QoS

特殊 VLAN

VLAN = 0、VLAN = 1 和 VLAN = 4095 与未标记 VLAN 的处理方式相同。 由于 VLAN 未标记，服务等级 (CoS) 不适用。

SIP 模式下的默认 QoS

如果 CDP 或 LLDP-MED 没有提供网络策略，则使用默认的网络策略。 CoS 基于指定分机的配置。 仅当手动 VLAN 已启用且手动 VLAN ID 不等于 0、1 或 4095 时才适用。服务类型基于特定分机的配置。

CDP 的 QoS 解决方案

若 CDP 中存在有效的网络策略：

- 如果 VLAN=0、1 或 4095，将不会设置 VLAN，或者 VLAN 未标记。 CoS 不适用，但 DSCP 适用。 ToS 基于上文所述的默认值。
- 如果 1 < VLAN < 4095，则会相应地对 VLAN 进行设置。 CoS 和 ToS 基于上文所述的默认值。 DSCP 适用。
- 电话将重新启动，并重新开始快速启动序列。

LLDP-MED 的 QoS 解决方案

如果 CoS 适用且 CoS=0，将如上文所述对特定分机使用默认值。 但是，用于传出 LLDPDU 的 TLV 的L2优先级上显示的值是基于用于分机1的值。如果COS适用且COS!=0，则COS用于所有分机。

如果 DSCP（映射到 ToS）适用且 DSCP=0，将如上文所述对特定分机使用默认值。 但是，用于输出 LLDPDU 的 TLV 的 DSCP 上显示的值是基于用于分机 1 的值。如果 DSCP 适用且 DSCP!=0，则 DSCP 用于所有分机 。

如果 1 < VLAN < 4095，则会相应地对 VLAN 进行设置。 CoS 和 ToS 基于上文所述的默认值。 DSCP 适用。

如果拥有针对来自 LLDP-MED PDU 的语音应用程序的有效网络策略且已设置带有标记的标志，则 VLAN、L2 优先级 (CoS) 和 DSCP（映射到 ToS）均适用。

如果拥有针对来自 LLDP-MED PDU 的语音应用程序的有效网络策略且未设置带有标记的标志，则只有 DSCP（映射到 ToS）适用。

Cisco IP 电话将重新启动，并重新开始快速启动序列。

与 CDP 共存

如果同时启用 CDP 和 LLDP-MED，则 VLAN 的网络策略会以两者中的一种发现模式确定所设置或更改的最后一个策略。 如果同时启用 LLDP-MED 和 CDP，则在启动期间电话会发送 CDP 和 LLDP-MED PDU。

在 CDP 和 LLDP-MED 模式下，如果网络连接设备的配置或行为不一致，可能导致电话振荡重启（因为会切换到不同的 VLAN）。

如果 CDP 和 LLDP-MED 未设置 VLAN，则使用手动配置的 VLAN ID。 如果没有手动配置的 VLAN ID，则不支持任何 VLAN。 如果适用，会使用 DSCP，并且网络策略会确定 LLDP-MED。

LLDP-MED 和多个网络设备

如果网络策略使用相同的应用程序类型，但电话从多个网络连接设备接收到不同的第 2 层或第 3 层 QoS 网络策略，则以最后接受的有效网络策略为准。 为确保网络策略的确定性和一致性，多个网络连接设备针对同一应用程序类型发送的网络策略不应相互冲突。

LLDP-MED 和 IEEE 802.X

Cisco IP 电话不支持 IEEE 802.X，无法在 802.1X 有线网络环境中使用。 但是，网路设备上的 IEEE 802.1X 或生成树协议可能会导致交换机快速启动响应延迟。